ANTI-TERRORISM INVESTIGATIONS AND THE FOURTH AMENDMENT AFTER SEPTEMBER 11, 2001

HEARING

BEFORE THE

SUBCOMMITTEE ON THE CONSTITUTION

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

MAY 20, 2003

Serial No. 35

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://www.house.gov/judiciary

U.S. GOVERNMENT PRINTING OFFICE

87–238 PDF WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*

HENRY J. HYDE, Illinois
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
SPENCER BACHUS, Alabama
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
MELISSA A. HART, Pennsylvania
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
JOHN R. CARTER, Texas
TOM FEENEY, Florida
MARSHA BLACKBURN, Tennessee

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SÁNCHEZ, California

PHILIP G. KIKO, *Chief of Staff-General Counsel*
PERRY H. APELBAUM, *Minority Chief Counsel*

SUBCOMMITTEE ON THE CONSTITUTION

STEVE CHABOT, Ohio, *Chairman*

STEVE KING, Iowa
WILLIAM L. JENKINS, Tennessee
SPENCER BACHUS, Alabama
JOHN N. HOSTETTLER, Indiana
MELISSA A. HART, Pennsylvania
TOM FEENEY, Florida
J. RANDY FORBES, Virginia

JERROLD NADLER, New York
JOHN CONYERS, JR., Michigan
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ADAM B. SCHIFF, California

CRYSTAL M. ROBERTS, *Chief Counsel*
PAUL B. TAYLOR, *Counsel*
D. MICHAEL HURST, JR., *Counsel*
MINDY BARRY, *Full Committee Counsel*
DAVID LACHMANN, *Minority Professional Staff Member*

CONTENTS

MAY 20, 2003

OPENING STATEMENT

WITNESSES

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

ANTI-TERRORISM INVESTIGATIONS AND THE FOURTH AMENDMENT AFTER SEPTEMBER 11, 2001

TUESDAY, MAY 20, 2003

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON THE CONSTITUTION,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:05 p.m., in Room 2141, Rayburn House Office Building, Hon. Steve Chabot (Chairman of the Subcommittee) presiding.

Mr. CHABOT. The Committee will come to order. This is the Subcommittee on the Constitution.

The Fourth Amendment provides that the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated. Our hearing today will consider the extent to which the implementation of the USA PATRIOT Act and some recent changes to the FBI's investigative guidelines comport with the Fourth Amendment and Fourth Amendment values.

In particular, the hearing will consider where and when the Federal Government can go to search the addressing information of electronic communications, library records, and public settings in order to prevent terrorist attacks.

The attacks on September 11 had a profound impact on our Nation and, in 1 day, changed the country's views on terrorism in many ways. In the wake of these tragic events, Congress stepped in and updated the law to fully engage in combatting terrorism by passing the USA PATRIOT Act. Changes to the law are still ongoing as current events unfold across the globe. Today, the threat of danger remains despite our military accomplishments in Afghanistan and Iraq. The recent deadly bombings in Israel, Morocco, and Saudi Arabia, and the raised terror alert in our country, show the need for law enforcement to be equipped with the tools to combat the threat of terrorism.

During the debate over the PATRIOT Act in the House, many of us in Congress, including myself, raised concerns about infringing on the civil liberties of the American people and, therefore, supported protective measures, such as the sunset. As we move forward in the process of providing the strong measures that are necessary to combat terrorism, we must also keep in mind the importance of protecting civil liberties Americans hold dear.

The Constitution Subcommittee gathers today to join the public debate regarding the balance between effective anti-terrorism measures and civil liberties, keeping in mind that one need not be the enemy of the other, while terrorism is the enemy of both.

Today, we meet to address several recent developments.

First, prior to the enactment of the USA PATRIOT Act, the Federal Government was allowed to access the numbers dialed on a telephone line if a Government attorney certified to the court that the information likely to be obtained is relevant to an ongoing criminal investigation. Although this authority allowed Government access only to numbers dialed on a telephone line, it has been used by the Department of Justice to obtain e-mail addresses, even if they contained only letters, names, or words, and no numbers.

The Department was doing so on the theory that while e-mail addresses are commonly referred to by names, such names are viewed by the computers as numbers because of the binary system of zeros and ones. Recognizing that such an argument could by its internal logic make the full substance of electronic communications accessible to the Government as digits, many were concerned at the time that the Government's retrieval of e-mail addresses was an unreasonably broad reading of the statutory terms.

The changes made by the USA PATRIOT Act made clear that addressing information of electronic communications could be obtained by the Government by explicitly authorizing the retrieval of dialing, routing, addressing, and signal information. However, the USA PATRIOT Act also strengthened privacy protections by clarifying that such addressing information obtained shall not include the contents of any communication. Further, the USA PATRIOT Act added new conditions on the use of so-called data-sniffing programs used by the FBI to gather electronic communications, including a requirement that records be maintained regarding how such programs are used, when they're used, how often they're used, and what they collect. Today we will examine whether the changes made by the USA PATRIOT Act regarding the Government's access to electronic addressing information have struck the proper balance.

Second, several of the September 11 terrorists used computers at public libraries to access the Internet. The USA PATRIOT Act updated the laws to make it more difficult for terrorists to use public places, including public libraries, to plot and carry out terrorist attacks. Prior to passage of the USA PATRIOT Act, FISA, the Foreign Intelligence Surveillance Act, empowered FISA courts to grant the FBI access to only certain business records, namely those in the custody of common carriers and businesses that provided public accommodations. The USA PATRIOT Act amended FISA such that any tangible item could be obtained with a FISA order—a term that can include library records. Today we will examine whether the changes made by the USA PATRIOT Act to the FISA law in this regard have struck the proper balance.

Third, terrorist organizations operating in this country have also used public places, including places of worship and public websites, as recruiting grounds and gathering places. Last year, changes were made to the FBI's internal guidelines that authorized FBI agents to visit any place and attend any event that is open to the

public on the same terms and conditions as members of the public generally. These changes have made information available to FBI agents on a par with local police and even young children accessing the Internet. Others, however, have argued that the knowledge that political activity at public events could be monitored by the Government will chill free speech without significant benefits. Today, we'll also examine whether these changes made to the FBI's internal guidelines have struck the proper balance.

When Congress was debating the USA PATRIOT Act, which would give law enforcement new tools to combat terrorism, we promised to conduct vigilant oversight over the implementation of these laws. This hearing today is a continuation of this important oversight, and we look forward to hearing from our witnesses here this afternoon.

I'll now yield to the gentleman from New York, Mr. Nadler, for his opening statement.

Mr. NADLER. Thank you, Mr. Chairman.

Today, we review the USA PATRIOT Act, legislation that was rushed into law in a manner that was, to say the least, not conducive to careful and thoughtful consideration. While the Members of our Committee worked cooperatively to forge legislation that won unanimous and bipartisan support—something rather unusual on this Committee—after, as I recall, a 4-day markup carefully considering amendments and carefully considering the balancing between privacy considerations and national security, the legislation that was ultimately signed into law bore little resemblance to the one we reported.

That legislation was drafted in secret over a weekend by representatives of the Department of Justice and the House leadership, was brought to the floor with no one having an opportunity to see it in advance. Members had to vote on a multi-hundred page bill, with no one having had a chance to even read the bill, except for staffs. The bill was available an hour in advance. People had to vote based on summaries.

This was shameful procedure to deal with legislation of such vital import and impact on our very liberties. When people said that we would have an opportunity to vet the legislation, to send it out to law schools and civil liberty unions and other groups that are interested for their comments, we were told that the ideas in this legislation had been around for a long time. True. Lots of ideas have been around for a long time. It doesn't make them good ideas. It also wasn't clear which ideas had gotten into the bill, the extent to which those ideas have gotten into the bill, the form those ideas had gotten into the bill. We were voting on the basic summaries. And we were told we didn't have time to consider the legislation properly because, if it were delayed by several days, lives could be lost.

With this kind of hysteria, the bill was passed almost sight unseen by the House, unfortunately. Now we are under—we are going to do the kind of oversight that we really should have done before voting on the bill. And it's about time we are. There were and have been bipartisan concerns that powers extended under the rubric of fighting terrorism, in fact allow Federal agencies to reach well beyond the war on terrorism to target the privacy and fundamental

liberties of average law-abiding Americans. Our witnesses today provide extensive evidence that the concerns of those who oppose this law as well as those who voted for it despite their misgivings have been borne out.

Of even greater concern is the extent to which this Administration's penchant for excessive secrecy has thwarted the Members of this Committee in the discharge of our constitutional duty to provide oversight of those activities within our jurisdiction and to monitor the strengths and weaknesses of the law and its implementation. I would hope that the Administration would be more responsive to congressional requests for specific rather than general information. "We can't tell you" or, in effect, "it's none of your business" are not adequate or acceptable answers to a congressional Committee seeking to exercise its legitimate oversight functions. While I do not often find myself in agreement with the Heritage Foundation, I think that we need to hear the—heed the warning Mr. Rosenzweig makes in his testimony on the need for careful and continuous congressional oversight.

Mr. Chairman, no one needs to instruct me about the dangers of terrorism or the need to fight it effectively. My District has been the target of repeated terrorist attacks, not only the September 11 attack on the World Trade Center, but on several occasions prior to that terrible day. Even now, there isn't a single New Yorker who's not acutely aware that when—not if—future acts of terror are attempted against this country, it will likely be our homes, our workplaces, our families, our neighbors, and our friends who will be at the top of the terrorist lists. No community has a greater stake in a successful war on terrorism than mine.

And yet, the—my constituents are consistently among the most outspoken defenders of individual rights in this war on terrorism. They do this not because they're indifferent to their own safety, but because they understand that the choice between liberty and safety is too often a false one. The abuse of power is never a substitute for effective police work. As Mr. Rosenzweig states in his prepared testimony, "Any new intrusion must be justified by a demonstration of its effectiveness in diminishing the threat."

It is not clear to me that targeting citizens or organizations without any basis for suspicion that they are engaged in illegal activity justifies a violation of their privacy or that it is necessarily the most effective way to provide for the safety and security of our Nation. I hope the Administration can reassure me on this point.

So Mr. Chairman, I look forward to the testimony of our panel. Liberty and security must not be partisan issues. They represent the fundamental underpinnings of the American way of life. We legislated in hysteria in October of 2001. We have done this before in times of crisis. It is now time for a sober second look. I want to commend you for scheduling this hearing.

I hope that we will be able to work together to provide consistent and effective oversight of this pressing and timely issue, and I hope that we can pass into law any necessary amendments that we find to be necessary as a result of these hearings. In particular, I'm interested in how the Administration can justify the kind of intrusive oversight, shall we say, of what people read in libraries that is in-

cluded in this act. And I look forward to your testimony—to their testimony. Thank you, Mr. Chairman.

Mr. CHABOT. Thank you. Do any other Members want to make opening statements? Mr. Jenkins? Mr. Scott? Any of the Members? Mr. Watt?

Mr. WATT. Thank you, Mr. Chairman. I'll be brief. I just wanted to take the opportunity to thank the Chairman for convening this hearing. I really can't think of a subject that cries out for a hearing more than the issue that's before us today. And I hope that this will be the first hearing and prelude to a full Committee hearing on this issue. And I hope, beyond that, that the Members of this House will use the information that is being submitted at this hearing and subsequent hearings to inform themselves better about how to strike an appropriate balance in these difficult times, and make sure that the constitutional imperatives are safeguarded.

I thank the Chairman for convening the hearing. I hope he will encourage the full Committee chair, as we have been doing, to have a follow-up hearing about the same issue. Thank you. Yield back.

Mr. CHABOT. Thank you. I would like to introduce the panel at this time, and we have a very distinguished panel this afternoon. I will start with our first witness, Viet Dinh. Mr. Dinh is assistant attorney general for the Office of Legal Policy at the Department of Justice. Prior to his entry into Government service, Mr. Dinh was professor of law and deputy director of Asian Law and Policy Studies at the Georgetown University Law Center. Mr. Dinh has also been a law clerk to Judge Lawrence Silverman of the U.S. Court of Appeals for the D.C. Circuit and to U.S. Supreme Court Justice Sandra Day O'Connor. We welcome you this afternoon, Mr. Dinh.

Our second witness is James Dempsey, the executive director of The Center For Democracy and Technology, where he works on privacy and electronic surveillance issues. Prior to joining the center, Mr. Dempsey was deputy director of the Center for National Security Studies. From 1985 to 1994, Mr. Dempsey was assistant counsel to this Subcommittee, where his primary areas of responsibility were oversight of the Federal Bureau of Investigation, privacy, and civil liberties. And we welcome you here this afternoon, Mr. Dempsey.

Our third witness is Orin Kerr, an associate law professor at the Georgetown Law—at the George Washington University Law School. Prior to his professorship, Mr. Kerr served for 3 years as a trial attorney in the Computer Crime and Intellectual Property Section of the Criminal Division at the U.S. Department of Justice. He has also served as a special assistant U.S. attorney for the Eastern District of Virginia, and since leaving the Government, he has worked on a pro bono basis as a criminal defense lawyer in computer crime cases. And we welcome you here this afternoon, Mr. Kerr.

And our final witness today is Paul Rosenzweig, a senior legal research fellow in the Center for Legal and Judicial Studies at the Heritage Foundation, where his research interests focus on issues of civil liberties and national security, criminal law, law enforcement, and legal ethics. Mr. Rosenzweig is also an adjunct professor of law at George Mason University School of Law. In addition, Mr.

Rosenzweig serves on the District of Columbia Bar Legal Ethics Committee. He has also served as senior litigation counsel in the Office of the Independent Counsel and in private practice. I want to thank you as well.

We thank you all for being here this afternoon. And as you probably know, we have a 5-minute rule. There are lights on the desk, and when the yellow light comes on, that gives you 1 minute to wrap up. And we'd appreciate it if you would conclude close to the red light.

We'll start with you, Mr. Dinh, and again, welcome to the Committee this afternoon.

STATEMENT OF VIET D. DINH, ASSISTANT ATTORNEY GENERAL FOR THE OFFICE OF LEGAL POLICY, DEPARTMENT OF JUSTICE

Mr. DINH. Thank you very much, Mr. Chairman. I thank you and the Ranking Member for having this meeting and for having me here. There has been much confusion, misinformation, and indeed sometimes disinformation about the events after September 11 or activities thereon, and I appreciate the opportunity to clear up some of the confusion.

I fully share Mr. Nadler's call for more public accountability and congressional information. That is why the department has been cooperating with this Committee and the full Committee on the questions on—with respect to oversight. In that respect, I call the Members' attention to the 60-page submission that we submitted last week containing information regarding our activities, about which I hope to have an opportunity to elucidate during this hearing.

Mr. Chairman, when the IRA failed in an attempt to assassinate British Prime Minister Margaret Thatcher in 1984, a spokesman said, "Today we were unlucky. But remember, we only have to be lucky once. You will have to be lucky always." That simple statement underscored the momentous task facing the Government after 9/11. Even as events in Saudi Arabia and Morocco this past week remind us that the terrorist threat is real and constant, we do take some comfort that terrorists have not successfully attacked the American homeland since September 11.

In our judgment, the successful effort in preventing another catastrophic attack on the American homeland in the past 20 months would have been much more difficult, if not outright impossible, without the tools that Congress has authorized, in particular, the tools in the USA PATRIOT Act. These authorities have substantially enhanced our ability to investigate, prosecute, and most important, to prevent terrorist attacks. In doing so, we are constantly mindful of the legal and constitutional limits to governmental authority. We have safeguarded the constitutional rights and civil liberties of law-abiding Americans, just as we have protected them from the threat of terror. We have achieved these twin objectives by implementing common-sense reforms and utilizing the tools that Congress has provided.

First, Congress has given us the legal authority to lower the artificial wall that divided the intelligence-gathering and law-enforcement functions of the FBI and the Department of Justice. Section

218 of the USA PATRIOT Act permitted the use of FISA authorities whenever "a significant purpose of the investigation is foreign intelligence." This simple change has permitted the transformation of our counterterrorism efforts, from the segregation of intelligence and law enforcement to a culture of cooperation and coordination.

Already this transformation has born fruit. The Department recently indicted Sami Al-Arian based on intelligence information that was previously denied to criminal investigators. Al-Arian is an alleged member of the Palestinian Islamic Jihad, which has allegedly engaged in terrorist killings of hundreds, including of Alisa Flatow, a young American killed in a bus bombing in the Middle East. At the direction of the Attorney General, criminal investigators in the Department are currently reviewing over 4,500 other intelligence files for information that may assist in the prosecution or prevention of terrorist crimes.

This dramatic transformation of our intelligence and law-enforcement culture comes at no cost to the civil rights and liberties of law-abiding citizens. Information on terrorist activities is collected according to established legal standards and its use in criminal trials is governed by the Constitution. Indeed, by making the most efficient use of information already gathered on terrorist activity, this transformation releases the pressure and reduces the demand for the Government to collect even more information.

Second, Congress has updated the law to the technology so that law enforcement no longer has to fight this 21st century war with antique weapons. Section 216 of the USA PATRIOT Act, for example, clarified—as you noted, Mr. Chairman—that courts can authorize the use of pen register devices to capture non-content routing and addressing information in electronic communications, just as they can to capture telephone numbers in analog telephone conversations.

This tool has been indispensable in our counterterrorism efforts. For example, in the Danny Pearl investigation, agents were able to use section 216 to obtain information that proved critical to identifying some of Pearl's killers, who now stand convicted in a Pakistani court of murder.

Again, Congress armed law enforcement with this powerful weapon without sacrificing the constitutional rights and civil liberties of law-abiding citizens. Of course, the Supreme Court has long held that non-content information is not protected by the Fourth Amendment, and section 216 extended this authority to the digital communications world by using the same legal predicate that existed in title III and in the analog world.

Third, and finally, we have authorized and motivated investigative agents to use their common sense and best judgment to prevent acts of terrorism. For decades, the Attorney General's guidelines centralized decision making and segregated information collected at field offices. We reversed this perverse arrangement so that street agents and their supervisors can collect the information and, once collected, transmit it to headquarters for proper analysis.

Mr. Chairman, the greatest present threat to the American people comes from the terrorists who seek to destroy our way of life. The men and women of law enforcement, instead, seek to protect that way of life and secure our liberty. The Department will con-

tinue to do everything in our power, with your help, to incapacitate the terrorists and to liberate the activities of law-abiding Americans. I thank you very much.

[The prepared statement of Mr. Dinh follows:]

PREPARED STATEMENT OF VIET D. DINH

Good afternoon, Mr. Chairman and Members of the Subcommittee. I appreciate the chance to testify today about the Justice Department's ongoing efforts to protect the lives of innocent Americans, and our commitment to doing so within the limits of the Fourth Amendment's guarantee of individual privacy. After 9/11, the Attorney General gave me a simple yet powerful directive: "Think outside the box, but never outside of the Constitution." Those instructions have been the Department's guidepost ever since.

In the 20 months since the atrocities of September 11, 2001, this Administration and Congress have worked hard to give our men and women in blue the tools they need to keep America safe, such as the USA PATRIOT Act and the revised Attorney General's investigative guidelines. Each of these new authorities incorporates long-settled precedent from the Supreme Court regarding privacy rights and other constitutional norms. In many cases, these new tools simply enable officials to use information to which other government entities already have access. In other instances, they give agents permission to use information that already is available to other members of the public.

This afternoon, I will discuss three matters that I hope will be of use to the Subcommittee. First, I will trace the development of Fourth Amendment jurisprudence to the contemporary understanding that it protects individual privacy. Second, I will discuss how the USA PATRIOT Act gave terrorism investigators access to information that other government officials already possess or lawfully could possess—in particular, how the Act encouraged the sharing of information and coordination among intelligence and law-enforcement personnel; and how the Act enabled courts to subpoena business records in all investigations, not just routine criminal cases. Third, I will discuss how the USA PATRIOT Act and Justice Department policies have enabled investigators to collect information that terrorism suspects voluntarily have disclosed to other members of the general public—in particular, how the revised Attorney General's investigative guidelines gave law enforcement the same access to public places and information that all other Americans enjoy; and how the Act facilitated the gathering of non-private routing and addressing information about electronic communications.

THE FOURTH AMENDMENT FROM TRESPASS TO PRIVACY

Over the course of the twentieth century, the Fourth Amendment came to be understood as protecting certain forms of individual privacy—what Justice Brandeis called the "right to be let alone—the most comprehensive of rights and the right most valued by civilized men"[1]—not just as preventing unauthorized government trespass onto landowners' private property.

The traditional "trespass" conception of the Fourth Amendment is typified by the 1928 case *Olmstead* v. *United States*.[2] In holding that law enforcement did not carry out an "unreasonable search or seizure" when it conducted a warrantless telephone wiretap, the Supreme Court reasoned that "[t]he evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants."[3] According to the Court, no trespass, no violation. But *Olmstead* also contained the seeds of a new understanding of the Fourth Amendment. In dissent, Justice Brandeis emphasized that "[s]ubtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet."[4]

Less than four decades later, in *Katz* v. *United States*,[5] the Supreme Court held that warrantless government wiretapping can constitute an unreasonable search or seizure. The Court effectively adopted Justice Brandeis's 'privacy" reading of the Fourth Amendment: "[T]he Fourth Amendment protects people, not places."[6] In re-

[1] *Olmstead* v. *United States,* 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).
[2] 277 U.S. 438 (1928).
[3] *Id.* at 464.
[4] *Id.* at 478 (Brandeis, J., dissenting).
[5] 389 U.S. 347 (1967).
[6] *Id.* at 351.

sponse to *Katz*, Congress enacted Title III of the 1968 Omnibus Crime Control and Safe Streets Act,[7] which governs electronic surveillance for federal criminal offenses. Congress subsequently enacted the Electronic Communications Privacy Act ("ECPA"), which addresses government access to stored communications,[8] and establishes statutory standards and procedures for the use of pen registers and trap and trace devices.[9]

Katz left open the question what standards and procedures apply to government surveillance in national-security investigations.[10] But in the 1972 *Keith* decision,[11] the Supreme Court squarely held that the Fourth Amendment is applicable in domestic-security investigations:

> We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be exercised in a manner compatible with the Fourth Amendment. In this case we hold that this requires an appropriate prior warrant procedure.[12]

At the same time, the *Keith* Court emphasized that different rules could be appropriate in national-security investigations—including cases of terrorism—than the standard procedures for criminal investigations:

> Given [the] potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens.[13]

In 1978, Congress responded to the Court's invitation by enacting the Foreign Intelligence Surveillance Act ("FISA").[14] FISA establishes standards applicable to surveillance of foreign powers and agents of foreign powers—including electronic surveillance, physical searches, and use of pen registers and trap and trace devices—in relation to the investigation of such matters as international terrorism and espionage.

FACILITATING INFORMATION SHARING AND AN INTEGRATED ANTITERRORISM CAMPAIGN

One of the USA PATRIOT Act's most important innovations was the amendments it made to FISA, which allow national-security personnel and their law-enforcement counterparts to coordinate their efforts to keep America safe. Acts of terrorism are simultaneously criminal offenses and threats to our national security. Our response likewise must transcend the boundaries of an organizational chart.

Before the USA PATRIOT Act, a metaphorical "wall" between the intelligence community and federal law enforcement often precluded vital information sharing. This wall, which derived from certain court decisions,[15] was established in written Department guidelines in July 1995. Under this interpretation, FISA could be used only if the "primary purpose" of an investigation was to protect the national security; evidence could be gathered to prosecute a foreign terrorist only if that purpose was clearly secondary. While information could be "thrown over the wall" from intelligence officials to prosecutors, the decision to do so always rested with national-security personnel—even though law enforcement agents pursuing a criminal investigation are in a better position to determine what evidence is pertinent to their case. These legal rules created what the Foreign Intelligence Surveillance Court of Review has termed "perverse organizational incentives," expressly discouraging co-

---

[7] 18 U.S.C. §§ 2510–22.
[8] *Id.* §§ 2701–12.
[9] *Id.* §§ 3121–27.
[10] *See Katz,* 389 U.S. at 358 n.23 ("Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case.").
[11] *United States* v. *United States District Court ("Keith")*, 407 U.S. 297 (1972).
[12] *Id.* at 320.
[13] *Id.* at 322.
[14] 50 U.S.C. §§ 1801–62.
[15] *See, e.g., United States* v. *Truong,* 629 F.2d 908 (4th Cir. 1980), cert. denied, 454 U.S. 1144 (1982).

operation in the fight against terrorism.[16] With apologies to Robert Frost, "[s]omething there is that doesn't love a wall."[17]

The USA PATRIOT Act finally permitted the coordination between intelligence and law enforcement that is vital to protecting the nation's security. Specifically, section 218 displaced the outmoded "primary purpose" standard, allowing the use of FISA when a "significant purpose" of an investigation is foreign intelligence. The Justice Department since has developed procedures to allow the use of certain FISA-derived information in criminal prosecutions. And on November 18, 2002 the FISA Court of Review held that these procedures are consistent with the Fourth Amendment, reasoning "that FISA as amended is constitutional because the surveillances it authorizes are reasonable."[18]

Both before and since the Court of Review's decision, the Justice Department has fostered extensive cooperation among national-security and law-enforcement personnel. The Attorney General instructed all United States Attorneys to review their intelligence files, with the intent of discovering whether there was a basis to bring criminal charges against the subjects of intelligence investigations. On October 1, 2002, the Attorney General directed every U.S. Attorney to develop a plan to monitor terrorism and intelligence investigations, and to ensure that information about terrorist threats is shared with other agencies and that criminal charges are considered. Almost 4,500 intelligence files have been reviewed as part of this process, and information from this review has been incorporated in numerous cases.

The USA PATRIOT Act's revisions to FISA already are producing important dividends in the war on terror. Department of Justice prosecutors recently were able to obtain the indictment of Sami al-Arian, an alleged member of a Palestinian Islamic Jihad (PIJ) cell in Tampa, Florida. PIJ is alleged to be one of the world's most violent terrorist outfits, and is responsible for murdering over 100 innocent people, including Alisa Flatow, a young American killed in a bus bombing near the Israeli settlement of Kfar Darom. Section 218 of the USA PATRIOT Act, as well as the Department's implementing rules, enabled criminal investigators finally to obtain and consider systematically the full range of evidence of the PIJ operations in which al-Arian allegedly participated.

ENABLING COURTS TO SUBPOENA RECORDS IN ALL TYPES OF INVESTIGATIONS

In the same way that national-security officers must be allowed to coordinate their antiterrorism efforts with law-enforcement personnel, the Department firmly believes that terrorism investigators must be able to use the same tools available in routine criminal investigations. For that reason, section 215 of the USA PATRIOT Act authorized courts in terrorism and national-security cases to subpoena business records—which have long been available in ordinary criminal investigations.

For years, grand juries investigating ordinary crimes have been able to issue subpoenas to all manner of businesses. In the 1997 Gianni Versace murder investigation, a Florida grand jury subpoenaed records from public libraries in Miami Beach.[19] In the Unabomber case during the mid-1990s, federal grand juries reportedly wanted to learn who had checked out the four books cited in the "Unabomber Manifesto," and therefore subpoenaed records from a number of university libraries on the west coast.[20] And in the 1990 Zodiac gunman investigation, a grand jury in New York subpoenaed records from a public library in an effort to learn who had checked out books written by a Scottish occult poet believed to be the gunman's inspiration.[21]

Section 215 simply authorized the FISA court to issue similar orders in national security investigations. These judicial orders conceivably could issue to bookstores or libraries but section 215 certainly does not single them out. The words "library" and "bookstore" appear nowhere in the USA PATRIOT Act. Nevertheless, libraries and bookstores should not be allowed to become safe havens for terrorists.

Moreover, the USA PATRIOT Act goes to great lengths to protect the privacy rights of libraries, other affected entities, and their patrons. First, the FBI cannot obtain records under section 215 unless it receives a court order. Agents cannot uni-

---

[16] *See In re* Sealed Case, 310 F.3d 717, 743 (FISCR 2002).

[17] Robert Frost, *Mending Wall, reprinted in* THE NEW OXFORD BOOK OF AMERICAN VERSE 395–96 (R. Ellmann ed. 1976).

[18] *Id.* at 746.

[19] *See* Lydia Martin, *Agents Seek Cunanan Link to Missing Library Book,* MIAMI HERALD, July 24, 1997, at A19.

[20] *See* Gary Marx and Peter Kendall, *Unabomber Path Leads back to Utah,* CHICAGO TRIBUNE, Sept. 25, 1995, at 1.

[21] *See Library Files Checked In Zodiac Investigation,* N.Y. TIMES, July 18, 1990, at B4.

laterally force people to turn over any information; they must appear before a court and convince it that they need the records.[22] Second, section 215 has an extremely narrow scope. It can only be used in international terrorism and espionage investigations; it is not available to investigate ordinary crimes, or even domestic terrorism.[23] Third, section 215 expressly protects the First Amendment, banning the FBI from using the exercise of First Amendment rights as a pretext for seeking records.[24] Fourth, and finally, section 215 provides for thorough congressional oversight. Every six months, the Attorney General is required to "fully inform" Congress on how it is being used.[25] The Justice Department furnished Congress with the required information most recently on December 31, 2002.

ALLOWING LAW ENFORCEMENT EQUAL ACCESS TO PUBLIC INFORMATION

FBI agents should have the same access to public places, events, and information that all other members of the general public enjoy. If terrorists open their meetings to the public, FBI agents ought to be able to accept the invitation. And if a child can use the internet to look up information that is relevant to potential terrorist activity, the FBI should be able to do the same. The revised Attorney General's investigative guidelines eliminated these counterproductive restrictions that prevented federal law enforcement from collecting information that was already in the public domain.

Under the old guidelines, there was no clear authority for agents to attend events held open to the general public—for example, meetings, speeches, and demonstrations—unless they already had obtained evidence that some sort of criminal activity was afoot. The old guidelines likewise generally barred the FBI from accessing publicly available information on the internet except when investigating a specific case. Thus, for example, during the fall 2001 anthrax investigation, an FBI agent might have been able to log on to an internet site to gather information about anthrax—but could not have accessed the same web page to gather information about another biotoxin such as smallpox.

The revised guidelines, issued in May 2002, represent a significant step forward in the war on terrorism. These new rules make explicit that an FBI agent may visit any public place to which members of the general public are invited, unless the Constitution or a federal law prohibits them from doing so, for the specific purpose of detecting or preventing terrorism:

> For the purpose of detecting or preventing terrorist activities, the FBI is authorized to visit any place and attend any event that is open to the public, on the same terms and conditions as members of the public generally. No information obtained from such visits shall be retained unless it relates to potential criminal or terrorist activity.[26]

The guidelines also strengthen the FBI's intelligence-gathering capabilities by making plain that agents may access public information online, even when not linked to a particular criminal investigation, for the purpose of detecting or preventing terrorism:

> The FBI is authorized to carry out general topical research, including conducting online searches and accessing online sites and forums as part of such research on the same terms and conditions as members of the public generally.[27]
>
> For the purpose of detecting or preventing terrorism or other criminal activities, the FBI is authorized to conduct online search activity and to access online sites and forums on the same terms and conditions as members of the public generally.[28]

The new guidelines contain a number of safeguards designed to preserve First Amendment, Fourth Amendment, and other constitutional norms. First, FBI agents may visit a public event or conduct internet research under the new authorizations only "on the same terms and conditions as members of the public generally."[29]

---

[22] *See* 50 U.S.C. § 1861(b)(1), (c)(1).
[23] *See id.* § 1861(b)(2).
[24] *See id.* § 1861(a)(1), (a)(2)(B).
[25] *Id.* § 1862.
[26] The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations, Part VI.A.2.
[27] *Id.* Part VI.B.1.
[28] *Id.* Part VI.B.2.
[29] *Id.* Part VI.A.2; *id.* Part VI.B.2.

Next, agents may conduct such visits only for a single, narrow purpose: "detecting or preventing terrorist activities."[30] Third, agents are expressly prohibited from keeping any information from these visits "unless it relates to potential criminal or terrorist activity."[31] Fourth, agents may not use these new authorities to keep files on people on the basis of their constitutionally protected activities.[32] Next, the guidelines stress that investigative activities may not be based solely on persons' exercise of their legal rights.[33] Sixth, and finally, the guidelines specifically order agents to comply with all relevant laws, including the Constitution, when conducting all investigations[34]

The revised Attorney General's guidelines fit comfortably within the Supreme Court's long-settled jurisprudence that there is no reasonable expectation of privacy in information voluntarily turned over to third parties. In fact, the Supreme Court has already held that government observation of public places is consistent with the First and Fourth Amendments. In *Laird* v. *Tatum*,[35] the Court held that the Army did not unconstitutionally "chill" the plaintiffs' exercise of their First Amendment rights by collecting publicly available information about potential insurrections and other civil disturbances. The Court found especially significant the fact that the Army gathered information from "the news media and publications in general circulation," as well as from "agents who attended meetings that were open to the public."[36] As is true under the new guidelines, "the information gathered is nothing more than a good newspaper reporter would be able to gather by attendance at public meetings and the clipping of articles from publications available on any newsstand."[37]

ENABLING THE COLLECTION OF NON-PRIVATE INFORMATION ABOUT INTERNET COMMUNICATIONS

Courts must be able to allow law enforcement to track the communications of terrorists regardless of which medium they choose to use. No one type of communication should be beyond the reach of court-approved, and Fourth Amendment sanctioned, surveillance. That is why section 216 of the USA PATRIOT Act has proven to be one of the most vital new authorities in the war on terrorism. Section 216 clarified that courts can authorize the use of "pen registers" and "trap and trace devices"—which track the numbers a particular telephone dials or receives—to obtain the same sort of routing and addressing information about internet communications. By law, pen/trap devices cannot be used to collect the content of communications.

Almost a quarter of a century ago, the Supreme Court squarely held, in the context of telephone surveillance, that the use of pen/trap devices does not constitute a "search" within the meaning of the Fourth Amendment. This is so because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," and "when he used his phone, petitioner voluntarily conveyed numerical information to the telephone company."[38] The same is true of internet communications, in which routing and addressing information is voluntarily disclosed to internet service providers. As a result, nothing in the Constitution requires law enforcement to establish probable cause, or obtain a court order, before using a pen/trap device. (Congress, by statute, has established procedural requirements that exceed those imposed by the Fourth Amendment.[39])

Since the USA PATRIOT Act became law in October 2001, Justice Department field investigators and prosecutors have used the amended pen/trap statute in a number of terrorism and other criminal cases. Section 216 was used in the investigation of the murder of *Wall Street Journal* reported Daniel Pearl, to obtain information that proved critical to identifying some of the perpetrators. It also has been used to collect routing information about the internet communications of (1) terrorist conspirators; (2) at least one major drug distributor; (3) thieves who obtained victims' bank account information and stole the money; (4) a four-time murderer; and (5) a fugitive who fled on the eve of trial using a fake passport.

Section 216 has proven as effective at safeguarding Fourth Amendment values as it has at bringing terrorists to justice. The USA PATRIOT Act preserved all pre-

[30] *Id.* Part VI.A.2
[31] *Id.*
[32] *Id.* Part VI.C.1
[33] *Id.* Part I.
[34] *Id.* Introduction, § C.
[35] 408 U.S. 1, 6 (1972).
[36] *Id.* at 6.
[37] *Id.* at 9 (citation omitted).
[38] *Smith* v. *Maryland,* 442 U.S. 735, 744 (1979).
[39] *See* 18 U.S.C. §§ 3121–27.

existing statutory standards: now, as before, law enforcement must get court approval before installing a pen register.[40] And now, as before, law enforcement must show that the information sought is relevant to an ongoing investigation.[41]

In fact, the USA PATRIOT Act's revisions to the pen/trap statute actually have *enhanced* privacy protections. The Act made explicit what was already implicit in the prior provision, namely, that an agency deploying a pen/trap has an affirmative obligation to use "technology reasonably available to it" that restricts the information obtained "so as not to include the contents of any wire or electronic communications."[42] The Act also made explicit that a pen/trap is not to be viewed as an affirmative authorization for the interception of content: "such information shall not include the contents of any communication."[43]

The Justice Department is committed to complying with the USA PATRIOT Act's mandate that law enforcement not use pen registers to capture the content of communications. On May 24, 2002, the Deputy Attorney General issued a memorandum to field offices instructing them on how to prevent "overcollection"—i.e., the inadvertent gathering of communication content—when using pen/trap devices. In particular, he ordered that:

(1) law enforcement must "operate a pen register or trap and trace device in a.manner that, to the extent feasible with reasonably available technology, will minimize any possible overcollection while still allowing the device to collect all of the limited information authorized";

(2) if "an agency's deployment of a pen register does result in the incidental collection of some portion of 'content,' it is the policy of this Department that such 'content' may not be used for any affirmative investigative purpose, except in a rare case in order to prevent an immediate danger of death, serious physical injury, or harm to the national security"; and

(3) "The Assistant Attorney General for the Criminal Division (AAG) should ensure that the Criminal Division provides appropriate guidance, through amendments to the United States Attorneys' Manual or otherwise, with respect to any significant general issues concerning what constitutes the 'content' of a communication."[44]

The Deputy Attorney General's directive will help guarantee effective implementation of section 216, while protecting the privacy of internet users by ensuring that only addressing information—and not the content of their communications—is collected and used.

The Justice Department's mission since the September 11 terrorist attacks has been as clear as it is essential: preserving the lives of innocent Americans along with the constitutional rights and liberties that make us as a people the envy of the world. In particular, we have dedicated ourselves to ensuring that all efforts to gather information about potential deadly terrorist attacks comply with the strictures of the Fourth Amendment's guarantee of individual privacy. Together with Congress, we have given investigators access to terrorism-related information that other governmental entities already have acquired, or lawfully could acquire. And we have enabled law enforcement to make use of information that can be retrieved by anyone in the public domain.

On behalf of the Administration, I thank you for your commitment to keeping America both safe and free, and we look forward to continuing our partnership. I would be happy to answer any questions that you may have.

Mr. CHABOT. Thank you. Mr. Dempsey?

You have to hit the button there.

STATEMENT OF JAMES X. DEMPSEY, EXECUTIVE DIRECTOR, THE CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. DEMPSEY. Thank you, Mr. Chairman. Good afternoon, Mr. Nadler, Members of the Subcommittee. Thank you for giving us the opportunity to testify today at this very important hearing. We

[40] *See id.* § 3123(a)(1).
[41] *See id.* § 3122(b)(2).
[42] *Id.* § 3123(c).
[43] *Id.* § 3127(3).
[44] Memorandum from Deputy Attorney General Larry D. Thompson Re: Avoiding Collection and Investigative Use of "Content" in the Operation of Pen Registers and Trap and Trace Devices, at 4–5 (May 24, 2002).

commend Members of this Subcommittee and Chairman Sensenbrenner and Mr. Conyers for the oversight that you have been pursuing into the application of the PATRIOT Act. This hearing is clearly just one step in that process.

I think that the answers to the questions that were submitted by the Justice Department—we just received them today, 69 pages—are another step. I'll say that in quickly looking at some of those, I have to say that some of them were not entirely clear answers and they raise additional questions, which, naturally, this Subcommittee and the full Committee will have to follow up on. We also received just today a 100-page report submitted by the Department of Defense in response to the Wyden-Grassley amendment on Total Information Awareness and data mining. So that's another form of congressional oversight that's now available to the public to help us understand how effective our laws are and their impact on civil liberties.

Undoubtedly, terrorism poses an imminent and grave threat to our society, and our Government needs the tools to fight this. But those tools need to be subject to checks and balances. They must be exercised with a focus on potential violence. They must be guided by the particularized suspicion requirement of the Fourth Amendment, which prohibits blanket searches. And they must be subject to executive, legislative, and judicial controls.

Yet before the PATRIOT Act, before 9/11, in our view, some of those checks and balances were weak and some of those controls were lacking. And the PATRIOT Act and other Executive Branch actions taken since then have brought us into a situation where the Government's powers are not well guided. And I think that is a problem both from an effectiveness standpoint, from a—from the standpoint of making us safer, as well as from the standpoint of constitutional rights.

I want to highlight just a few items and then respond to your more detailed questions. Specifically on the question of libraries, which Mr. Nadler raised, libraries are not a law-free zone. They should not be a haven for terrorists. They never were. The question has always been what is the standard that the Government needs to follow in order to get information from a library or from other—any other entity. And in the PATRIOT Act, really, the standards that had been in place, which required some reason to believe that there was some connection with terrorism and some minimal factual showing, some relationship to an individual, those standards were eliminated. And now, the so-called section 215 of the PATRIOT Act and the so-called national security letter authorities, at least to my reading, seem to allow the Government to get entire databases—not to go in and ask for the books that a terrorist has read, but to ask for the books that everybody has read—or the suspected terrorists, but to ask for the books read by everybody.

Assistant Attorney General Dinh has mentioned the changes to the Foreign Intelligence Surveillance Act. We are now going to be seeing more information acquired under FISA used in criminal cases, and in many respects that's appropriate. But when that information is used, it should be subject to the normal criminal due process rules. And right now, defendants facing FISA evidence in court do not enjoy the same rights that a defendant normally en-

joys in dealing with wiretap information collected under the title 3 criminal wiretap law.

The pen register trap and trace statute, the statute that allows the collection of transactional information—dialed number information or e-mail addressing information—perfectly appropriate that the Government should have laws that keep up with the technology to acquire that information when justified, but the law as it now stands really doesn't have any standards in it. It says that Government can get one of those orders just upon the certification of a prosecutor that it is relevant to an ongoing investigation. No factual inquiry at all by the judge. The judge, really, just becomes a rubber stamp. That information is good, it's useful, but it should be subject to standards.

Similarly, there should be tighter standards on the use of secret searches which were authorized in the PATRIOT Act. The whole question of data mining, which is now a major subject in the news, we just don't have the laws that are applicable to that. The Privacy Act doesn't apply and other laws do not apply.

So we really need to put these protections in place, and if we do, I believe that they actually do not limit counterterrorism effectiveness. These are things that help guide it and focus it and make it more effective. And I think we can do that in a way that makes us safer without sacrificing civil liberties.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Dempsey follows:]

PREPARED STATEMENT OF JAMES X. DEMPSEY

Mr. Chairman, Mr. Nadler, Members of the Subcommittee, thank you for the opportunity to testify today at this important hearing. We commend Chairman Sensenbrenner and Mr. Conyers and you, Chairman Chabot and Mr. Nadler, for the oversight you are conducting of the effectiveness of the nation's counter-terrorism laws and their implications for civil liberties. The Center for Democracy and Technology [1] urges you to continue this process, and we look forward to being of assistance to you however we can. In my testimony today, I make specific suggestions for further avenues of oversight.

I. SUMMARY

The main points I wish to make today are these: The threat terrorism poses to our nation is imminent and grave. The government must be provided with strong legal authorities to prevent terrorism to the greatest extent possible and to punish it when it occurs. These authorities must include the ability to infiltrate organizations, collect information from public and private sources, and carry out wiretaps and other forms of electronic surveillance. These legal powers, however, must be subject to checks and balances; they must be exercised with a focus on potential violence, guided by the particularized suspicion principle of the Fourth Amendment, and subject to Executive, legislative and judicial controls. Yet the checks and balances, weak in some key respects before 9/11, have been seriously eroded by the PATRIOT Act and Executive Branch actions. Prior to 9/11, the government had awesome powers but failed to use them well. Those failures had little if anything to do with the rules established to protect privacy. The changes in the PATRIOT Act were hastily enacted—mistakes were made that Congress should rectify, by reasserting standards and checks and balances and by practicing ongoing, nonpartisan, detailed oversight, starting with close scrutiny of the government's claims that the PATRIOT Act changes have been vital to recent successes.

[1] The Center for Democracy and Technology is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values for the new digital communications media. Our core goals include enhancing privacy protections and preserving the open architecture of the Internet. Among other activities, CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications, and public interest organizations, companies and associations interested in information privacy and security issues.

In response to the specific question posed by the title of this hearing, my central point is that, both before 9/11 and now, the government had and still has authority to go anywhere and collect any information to prevent terrorist attacks. Before 9/11, the exercise of that authority domestically was controlled and focused—the government had to have some minimal basis to suspect that some criminal conduct was being planned or that there was some minimal connection with a foreign terrorist group. Under the changes that have been made since 9/11, the FBI is authorized by the Attorney General to go looking for information about individuals with no reason to believe they are engaged in, or planning, or connected to any wrongdoing. Before 9/11, mosques and political events were not off-limits and the FBI did go into religious and political gatherings to collect information—where it had some minimal reason for believing that there was some connection between that mosque or political meeting and terrorism. Now, FBI agents can apparently wander down the street and visit mosques or political meetings like anyone else—on a whim. Before 9/11, the FBI was not prohibited from use of commercial databases. But under the PATRIOT Act and other laws, the FBI may have the authority to scoop up entire databases of information, including data on persons suspected of no wrongdoing. Our laws are totally inadequate to deal with the reality of decentralized commercial databases and the new techniques of data mining.

Both before 9/11 and today, the only question has ever been one of standards, checks and balances and procedures. With the changes adopted since 9/11, domestic law enforcement and intelligence agencies have fewer standards to guide them and are subject to less oversight and accountability to check up on their performance. The result, I fear, is unfocused investigative activity that is bad for security and bad for civil liberties.

I will concentrate today on the surveillance issues that I understand are the Subcommittee's main interest, but for purposes of context, I must briefly mention that some of the greatest abuses of civil liberties since 9/11 do not flow from the PATRIOT Act and have not been the subject of Congressional authorization or scrutiny, including:

- secret arrests of hundreds and maybe more than 1000 people;
- the detention of many of those for days, weeks or even longer without charges, even though Congress had set a 7 day limit even for non-citizens detained as suspected terrorists;
- abuse of the material witness statute to hold people without charges;
- the blanket closing of deportation hearings;
- the indefinite detention of two American citizens in military prisons without criminal charges;
- selective targeting of immigrants for enforcement based on their religion.[2]

II. *U.S.* V. *MILLER* AND THE DRAGNET APPROACH OF SECTION 215 AND NATIONAL SECURITY LETTERS

In the 1970s, the Supreme Court issued a series of momentous decisions holding that citizens lose their constitutional rights in information provided to third parties in the course of commercial transactions. *United States* v. *Miller*, 425 U.S. 435 (1976), held that there is no constitutional privacy interest in the records held by banks showing who has paid you money, to whom you have paid money, amounts, dates, etc. *Smith* v. *Maryland*, 442 U.S. 735 (1979), held that telephone users have no constitutional privacy interest in the transactional information that shows who is calling them, whom they are calling, when, how often and for how long. Fast forward through the digital revolution, and the "business records" exception has become a gaping hole in the Fourth Amendment. Under current law, you have no constitutional privacy right in any of the data you generate as you go about your daily life, using credit cards, building access cards, or Easy Passes, making travel plans, or buying things. Taken together, the transactional data generated every time you dial your telephone, write a check, send an email, or go to the doctor can provide a full picture of your life, your work, your interests and your associations, but it is, under current law, constitutionally unprotected.

The PATRIOT Act exploited this situation, granting broad authorities beyond anything contemplated in *U.S.* v. *Miller* or *Smith* v. *Maryland*. Section 215 of the Act amended the Foreign Intelligence Surveillance Act to authorize the government to

[2] Many of these abuses are detailed in the report of the Lawyers Committee for Human Rights, "Imbalance of Powers: How Changes to U.S. Law and Policy since 9/11 Erode Human Rights and Civil Liberties," [PDF] March 11, 2003, online at *http://www.lchr.org/us—law/loss/imbalance/powers.pdf.*

obtain a court order from the FISA court or designated magistrates to seize "any tangible things (including books, records, papers, documents, and other items)" that an FBI agent claims are "sought for" an authorized investigation "to protect against international terrorism or clandestine intelligence activities." The subject of the order need not be suspected of any criminal wrongdoing whatsoever; indeed, if the statute is read literally, the order need not name any particular person but may encompass entire collections of data related to many individuals. Section 505 of the PATRIOT Act similarly expanded the government's power to obtain telephone and email transactional records, credit reports and financial data with the use of a document called the National Security Letter (NSL), which is issued by FBI officials without judicial approval.[3] Sections 507 and 508 granted authority to the Attorney General or his designee to obtain a court record for disclosure of education records.

In the past, the government could obtain a person's records from a bank, credit bureau, telephone company, hospital, or library in the course of a criminal investigation. In addition, prior to the PATRIOT Act, in international terrorism investigations, the FBI had the power to compel disclosure of credit, financial and communications records with National Security Letters and travel records under the predecessor of Section 215. However, Congress had set a straightforward and relatively low standard that required some factual predicate and particularized focus: the government had to have reason to believe that the records being sought pertained to an "agent of a foreign power"—an intelligence officer, for example, or a member of an international terrorist organization. Reason to believe is a very low standard, much lower than probable cause.

The PATRIOT Act eliminated both the "agent of a foreign power" standard and the reason to believe standard, giving the FBI access with National Security Letters to specific categories of records in intelligence investigations with no factual basis to believe that the records pertained to a possible terrorist. And Section 215 created a massive catch-all provision that gave the FBI the ability to compel anyone to disclose any record or tangible thing that the FBI claims is "sought in connection with" an investigation of international terrorism or "clandestine intelligence activities," even if the record does not pertain to a suspected spy or international terrorist.

The implications of this change are enormous. Previously, the FBI could get the credit card records of anyone suspected of being a foreign agent. Under the PATRIOT Act, broadly read, the FBI can get the entire database of the credit card company. Under prior law, the FBI could get library borrowing records only with a subpoena in a criminal investigation, and generally had to ask for the records of a specific patron. Under the PATRIOT Act, broadly read, the FBI can go into a public library and ask for the records on everybody who ever used the library, or who used it on a certain day, or who checked out certain kinds of books. It can do the same at any bank, telephone company, hotel or motel, hospital, or university—merely upon the claim that the information is "sought for" an investigation to protect against international terrorism or clandestine intelligence activities.

How these provisions are actually being applied is the subject of great uncertainty, at least as far as one can tell from the public discussion to date. The DOJ and the FBI could be much more forthcoming, for example, about what they are doing in libraries. Up to now, the ambiguous statements of FBI officials have only fanned suspicion and distrust.

Congress should closely inquire into the DOJ's interpretation of Section 215 and the National Security Letter authorities. The DOJ and FBI have never actually said how they are interpreting Section 215 and the new NSL authorities. The further questions submitted by Chairman Sensenbrenner on April 1, 2003 are a good start, but the Committee should also ask: Is the DOJ interpreting and using Section 215 and the NSL authorities to obtain access to entire databases, i.e., without naming individuals to whom the records pertain? If not, why shouldn't the statute be revised to clarify the particularized suspicion standard?

I have heard it argued that these changes merely conform the intelligence standard to the criminal standard, since investigators in criminal cases can obtain anything with a subpoena issued on a relevance standard. First of all, the standard in Section 215 and two of the three NSL statutes is less than relevance—it is "sought for." Second, a criminal case is at least cabined by the criminal code—something is relevant only if it relates to the commission of a crime. But on the intelligence side, the government need not be investigating crimes—at least for non-U.S. persons, it can investigate purely legal activities by those suspected of being agents of foreign powers. The standard for opening an investigation is far less than probable cause,

[3] CDT has prepared a detailed memo on data mining, which discusses Section 215 and the NSLs: "Privacy's Gap: The Largely Non-Existent Legal Framework for Government Mining of Commercial Data," May 19, 2003, available online at *http://www.cdt.org.*

and once an investigation is opened, under the PATRIOT Act changes, an agent can get anything from anyone by say "I am seeking this in connection with an open investigation."

Moreover, there are other crucial protections applicable to criminal subpoenas that are not available under Section 215 and the NSLs. For one, third party recipients of criminal subpoenas can notify the record subject, either immediately or after a required delay. Section 215 and the NSLs prohibit the recipient of a disclosure order from ever telling the record subject, which means that the person whose privacy has been invaded never has a chance to rectify any mistake or seek redress for any abuse. Secondly, the protections of the criminal justice system provide an opportunity for persons to assert their rights and protect their privacy, but those adversarial processes are not available in intelligence investigations that do not end up in criminal charges.

I look forward to the day when *Smith* v. *Maryland* and *U.S.* v. *Miller* are placed in the same category as the discredited *Olmstead* decision of 1928—decisions based on an unduly cramped understanding of privacy, unsuited to changing technology. *Kyllo* v. *United States*, 533 U.S. 27 (2001), the case requiring a warrant for infrared searches of homes, showed that the Supreme Court is sensitive to ensuring that changes in technology do not render privacy. Meanwhile, Congress should statutorily re-establish the requirement of particularized suspicion and require some factual showing on the part of government officials seeking access to records.

III. THE NEED FOR CLOSE CONGRESSIONAL SCUTINY OF THE EFFECTIVENESS AND PRIVACY IMPLICATIONS OF DATA MINING AND ESTABLISHMENT OF GUIDELINES FOR ANY APPLICATION OF THE TECHNOLOGY

One important avenue of oversight for this Committee is how the FBI intends to use the technique known as data mining, which purports to be able to find evidence of possible terrorist preparations by scanning billions of everyday transactions, potentially including a vast array of information about Americans' personal lives such as medical information, travel records and credit card and financial data. The FBI's Trilogy project includes plans for data mining. According to an undated FBI presentation obtained by the Electronic Privacy Information Center, the FBI's use of "public source" information (including proprietary commercial databases) has grown 9,600% since 1992.[4]

Two kinds of questions must be asked about data mining. First, is the technique likely to be effective? Secondly, assuming it can be shown to be effective, what should be the rules governing it? This week, the Defense Department will be releasing a report on the Total Information Awareness ("TIA") project at the Pentagon's Defense Advanced Research Projects Agency ("DARPA"), which hopefully will illuminate some of these issues. Among the questions to be asked specifically of the FBI is how the PATRIOT Act authorities discussed above and the changes in the FBI guidelines discussed below might relate to its data mining plans.

Current laws place few constraints on the government's ability to access information for terrorism-related data mining. Under existing law, the government can ask for, purchase or demand access to most private sector data. Unaddressed are a host of questions: Who should approve the patterns that are the basis for scans of private databases and under what standard? What should be the legal rules limiting disclosure to the government of the identity of those whose data fits a pattern? When the government draws conclusions based on pattern analysis, how should those conclusions be interpreted? How should they be disseminated and when can they be acted upon?

Adapting the Privacy Act to government uses of commercial databases is one way to look at setting guidelines for data mining. But some of the principles are simply inapplicable and others need to have greater emphasis. For example, perhaps one of the most important elements of guidelines for data mining would be rules on the interpretation and dissemination of hits and on how information generated by computerized scans can be used. Can it be used to conduct a more intensive search of someone seeking to board an airplane, to keep a person off an airplane, to deny a person access to a government building, to deny a person a job? What due process rights should be afforded when adverse actions are taken against individuals based on some pattern identified by a computer program? Can ongoing audits and evaluation mechanisms assess the effectiveness of particular applications of the technology and prevent abuse?

All of these questions must be answered before moving forward with implementation. Congress should limit the implementation of data mining until effectiveness

[4] *http://www.epic.org/privacy/publicrecords/cpfbippt.pdf.*

has been shown and guidelines on collection, use, disclosure and retention have been adopted following appropriate consultation and comment.

IV. THE FBI GUIDELINES: IMPACT ON CIVIL LIBERTIES AND SECURITY—THE NEED FOR CONGRESSIONAL OVERSIGHT AND RE-ESTABLISHMENT OF MEANINGFUL LIMITS

On May 30, 2002, Attorney General John Ashcroft issued revised Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations ("Domestic Guidelines"). The Attorney General claimed that the changes were necessary to free the FBI from unnecessary constraints in the fight against international terrorism. Yet the guidelines the Attorney General changed were not applicable to international terrorism. And the types of things the Attorney General said he wanted to permit—visiting mosques, surfing the Net—were never prohibited under the old guidelines.

The FBI is subject to two sets of guidelines, a classified set for foreign intelligence and international terrorism investigations ("International Terrorism Guidelines"), and an unclassified set on general crimes, racketeering and domestic terrorism.[5] Last year, the Attorney General changed the Domestic Guidelines. He has not yet changed the International Guidelines, which relate to investigations of Osama bin Laden and Al Qaeda. (The Department of Justice may be reviewing the International Guidelines. This Committee should find out what is going on and insist on being fully consulted.) The International Terrorism Guidelines in some ways give the FBI even more latitude than the domestic guidelines. The irony is that the FBI's failed investigations of the Osama bin Laden group were conducted under those looser guidelines, reinforcing the conclusion that the problem before 9/11 was not the limits imposed by law or policy but the failure of the FBI to use the authority and information it already had.

—The Role of Congress

In the 1960s, the FBI conducted wide-ranging investigations and neutralization efforts against non-violent activity across the political spectrum. While there were acts of violence being carried out on America's streets, the FBI's COINTELPRO program and related efforts focused on politics. The exercise was essentially worthless from a security standpoint: it produced no advanced warning of any violent activity. By the mid-70s, there was a reaction against this approach, within the Justice Department, the FBI itself, the Congress and the public at large. Internal and external investigations of the abuses led to the adoption of guidelines by Attorney General Edward Levi, which set standards for FBI "domestic security" investigations.

The initial issuance and subsequent major revisions of the FBI Guidelines were undertaken in conjunction with Congressional consultation and oversight. In effect, the Guidelines had a "quasi-legislative" status. Indeed, the Guidelines were adopted in lieu of legislation. A major debate in the 1970s was over the framing of a statutory charter for the FBI. (The CIA has a legislative charter; the FBI does not.) After Attorney General Levi issued the guidelines, Congress dropped the push for a legislative charter, based on two grounds: (i) Executive Branch claims that the guidelines embodied all the protections that would be included in a charter but did so with greater detail, providing just the right mix of guidance and flexibility to the FBI, and (ii) the understanding that Guideline changes would be subject to prior Congressional review and public input. Every subsequent Attorney General (except Attorney General Ashcroft) consulted with this Committee on guidelines changes. When Attorney General William French Smith undertook major revisions of the guidelines at the beginning of the Reagan Administration, the effort was accompanied by over a year of consultation, public debate, and Congressional hearings. Never before has an Attorney General undertaken major revisions to the FBI Guidelines without any prior consultation with the relevant Committees of Congress.

—Major Concerns with the Changes

A major change brought about by the Ashcroft Guidelines is that they authorize investigative activity in the absence of any indication of criminal conduct. The central feature of the Levi/Smith/Thornburgh guidelines was the criminal standard: the

---

[5] The old domestic guidelines are at *http://www.usdoj.gov/ag/readingroom/generalcrimea.htm*. A heavily redacted copy of the international guidelines can be downloaded in PDF from *http://www.usdoj.gov/ag/readingroom/terrorismintel2.pdf*. Both sets of guidelines relate to investigations in the United States. The difference between the two sets of guidelines has to do with the nature of the organization being investigated. The foreign guidelines govern investigations inside the United States of international terrorism organizations (such as al Qaeda or Hamas), groups that originate abroad but carry out activities in the U.S., and their agents. In the past, the domestic guidelines governed investigations of terrorist groups that originate in the U.S.—e.g., white supremacists and animal rights activists.

FBI could initiate a full domestic counter-terrorism investigation when facts and circumstances reasonably indicated that two or more people were engaged in an enterprise for the purpose of furthering political goals through violence. FBI agents could conduct quite intrusive preliminary investigations on an even lower standard. The old guidelines allowed FBI agents to go into any mosque or religious or political meeting if there was reason to believe that criminal conduct was being discussed or planned there, and, in fact, over the years the FBI conducted terrorism investigations against a number of religious organizations and figures, ranging from the white supremacist Christian Identity Movement to the African-American Church of Yahweh. Separate guidelines even allowed undercover operations of religious and political groups, subject to close supervision.

Under the Levi/Smith/Thornburgh guidelines, once an investigation or even a preliminary inquiry was opened, the FBI could use any and all public source information (including the Internet) to collect personally-identifiable information relevant to the investigation. In fact, an investigation could consist solely of the collection of newspaper articles and Internet material and the indexing of that information by name. The evidence could in fact consist largely or exclusively of information about the exercise of First Amendment rights. The only requirement was that there first had to be some minimal reason to believe that something illegal was being planned.

Now, the FBI is cut loose from that standard, with no indication as to how it should prioritize its efforts or avoid chilling First Amendment rights.

Visiting Religious and Political Meetings—The new guidelines purport to give the FBI authority to attend public meetings of a religious or political nature, without any scintilla of suspicion of criminal or terrorist activity. The problem is compounded by poor guidance on what can be recorded and the lack of time limits on the retention of data acquired.

In the past, under the Domestic Guidelines, the FBI was guided by the criminal nexus—in deciding what mosques to go to and what political meetings to record, it had to have some reason to believe that terrorism might be discussed. Under the new guidelines, even before opening a preliminary inquiry, the FBI can go to mosques and political meetings. How will it decide which ones to go to? We fear it will be on the basis of politics, religion, or ethnicity.

Should FBI Agents Surf the Net Like Teenagers?—According to justifications issued by the DOJ with the new guidelines, FBI agents previously could not conduct online searches under the term "anthrax," even after the initial appearance of the anthrax letters. That is absurd—there was an ongoing investigation. Anyhow, no privacy rights or civil liberties are implicated in searches—before or after the appearance of the anthrax letter—for words like "anthrax." That is not what the guidelines were about. The question is whether the FBI can make searches for "Palestinian rights" or other terms with a political, ethnic or religious significance, as the starting point for an investigation. The change either authorizes politically guided investigations or it authorizes fishing expeditions

Pursuing Investigations That Turn Up Nothing—Finally, the revisions decreased the internal supervision and coordination at various stages of investigation, in particular expanding the scope and duration of preliminary inquiries (by definition, these are cases that are opened on less than reasonable indication of criminal or terrorist conduct), encouraging the use of more intrusive techniques with no sense of prioritization and allowing intrusive investigations to go on for periods without producing results and without internal review or any outside or independent scrutiny.[6]

Preliminary inquiries can use all techniques except two: mail openings and wiretaps. This means that the FBI can use informants, Internet searches, undercover operations, and physical and photographic surveillance. Under the old guidelines, if 90 days of investigation turned up no indication of criminal activity, the investigation could be continued only with HQ approval. Under the new guidelines, preliminary inquiries can continue 1 year without HQ approval. This means that the FBI can conduct an investigation, using highly intrusive techniques, for one year (and longer with HQ approval) even if the investigation is turning up no reasonable indication of criminal activity.

---

[6] The period for preliminary inquiries with no supervisory review has increased from 90 to 180 days. Preliminary inquiries may go on for up to one year without notifying Headquarters. While the time limitations have increased, the levels of authorization have decreased. Authority for extensions in preliminary inquiries - cases that are producing no reasonable indication of criminal conduct - has been reduced from FBI Headquarters to a Special Agent in Charge. Likewise, authority for the initiation and review of full investigations has been reduced from a Director or Assistant Director to a Special Agent in Charge.

Broadening the FBI's surveillance authority threatens civil liberties and wastes resources while increasing the risk of intelligence failures. The salient identifiable cause of the September 11 intelligence failure was the inability of the FBI and other agencies to use the information they already had. The guidelines are likely to compound that defect, thereby producing no improvement in security.

—*Congressional Oversight is Necessary*

Consistent Congressional oversight is vital to protect our security and our civil liberties. Attorney General Ashcroft changed the FBI Guidelines with the stroke of a pen without prior notice or consultation with Congress. This is not only unprecedented, but does not bode well for Congressional oversight over FBI activity to ensure both protection of constitutional rights and success in the fight against terrorism.

In responding to the issues raised by the guideline changes, we recommend the following steps:

- Require through appropriations language prior notice and meaningful consultation before future guideline changes can take effect, including changes in the International Guidelines
- Require the adoption, following Congressional consultation and comment, of Guidelines for collection, use, disclosure and retention of public event information. Such guidelines should include a provision specifying that no information regarding the First Amendment activities of a U.S. person or group composed substantially of U.S. persons can be disseminated outside the FBI except as part of a report indicating that such person or group is planning or engaged in criminal activity.
- Provide resources and authority to the General Accounting Office and the DOJ Inspector General to collect and analyze information on implementation of the anti-terrorism guidelines and to submit to Congress public and classified reports on their impact on an open society, free speech, and privacy and benefits and costs to national security.

V. RECTIFYING FLAWS IN THE SURVEILLANCE LAWS

We should not loose sight of the fact that before the PATRIOT Act there were concerns that the checks and balances in the surveillance laws were insufficient. As a result of the digital revolution more information is more readily available to government investigators than ever before. The judges have not aggressively regulated electronic surveillance. Last year, only one government application for electronic surveillance was turned down. For each of the prior three years (1999–2001), not a single judge anywhere in the country, state or federal, turned down a single request for surveillance in any case, criminal or intelligence. The minimization requirement has been judicially eviscerated. The Congress could start by taking up the helpful changes to surveillance law developed and passed by the House Judiciary Committee in the 106th Congress, under H.R. 5018, including:

- Heightened protections for access to wireless location information, requiring a judge to find probable cause to believe that a crime has been or is being committed. Today tens of millions of Americans are carrying (or driving) mobile devices that could be used to create a detailed dossier of their movements over time—with little clarity over how that information could be accessed and without an appropriate legal standard for doing so.
- A meaningful standard for use of expanded pen registers and trap and trace capabilities, requiring a judge to at least find that specific and particularly facts reasonably indicate criminal activity and that the information to be collected is relevant to the investigation of such conduct.
- Addition of electronic communications to the Title III exclusionary rule in 18 USC § 2515 and add a similar rule to the section 2703 authority and the pen register and trap and trace authority. This would prohibit the use in any court or administrative proceeding of email or other Internet communications intercepted or seized in violation of the privacy standards in the law.
- Require high-level Justice Department approval for applications to intercept electronic communications, as is currently required for interceptions of wire and oral communications.
- Require statistical reports for § 2703 disclosures, similar to those required by Title III.

Beyond these changes, there are issues raised by the PATRIOT Act that need to be addressed:

- Require more extensive public reporting on the use of FISA, to allow better public oversight.
- Make the use of FISA evidence in criminal cases subject to the Classified Information Procedures Act.
- Limit the use of secret searches.

Conclusion

We need limits on government surveillance and guidelines for the use of information not merely to protect individual rights but to focus government activity on those planning violence. The criminal standard and the principle of particularized suspicion keep the government from being diverted into investigations guided by politics, religion or ethnicity. Legal standards should focus on perpetrators of crime, avoid indulging in guilt by association, maintain procedures designed to identify the guilty and exonerate the innocent, insist on limits on surveillance authority, and bar political spying.

Mr. CHABOT. Thank you very much. Our next witness will be Mr. Kerr. Professor Kerr.

STATEMENT OF ORIN KERR, ASSOCIATE LAW PROFESSOR, GEORGE WASHINGTON UNIVERSITY LAW SCHOOL

Mr. KERR. Thank you, Mr. Chairman and Members of the Subcommittee, for the opportunity to testify today.

Before 9/11 2001, there were a bunch of pretty esoteric laws on the books, such as the Electronic Communications Privacy Act and the Foreign Intelligence Surveillance Act, and few people understood them well and many people didn't even know they existed. Following 9/11 and following the PATRIOT Act, these are the laws that are now on the front page of the paper, putting this Congress in the difficult and very important position of coming up with the right set of rules that should govern the Executive Branch in its investigations, criminal investigations and counterintelligence terrorism investigations, both online and off, made all the more important and real by the attacks of 9/11.

The difficult challenge, of course, is to navigate some sort of middle ground between two clearly undesirable alternatives. Give the Executive Branch too much power, and it enables abuses which could violate our civil liberties. Give the Government too little power, and it disables the Government from protecting the public from the threat of both terrorism and crime. This issue is made all the more important for Congress because the courts have generally proven relatively deferential—for example, in deciding that the Fourth Amendment does not protect any addressing information of either Internet or, or non-Internet communications—making those standards, really, something that is up to the Congress.

Yet another challenge in this area is that the press has often had a hard time explaining what these very complicated laws do, so oftentimes the newspapers will say the law's doing one thing, when in reality the stories have gotten it slightly off, still posing very difficult challenges for the Congress to find that balance in a way that reflects what the laws are actually doing, often requiring a great deal of scrutiny of very difficult statutory texts that can go on for many pages.

One example of a change to surveillance laws which I think is a positive one, although only a partial step toward the right solution, brought about by the PATRIOT Act, is section 216 of the PATRIOT Act, which clarifies that the pen register law, a 1986 law,

applies as well to the Internet. That's a law which was designed to apply to the telephone, and it protects the privacy of telephone communications addressing information; for example, the numbers dialed on the telephone. Prior to the PATRIOT Act, it was simply unclear whether that law also protected Internet communications or whether non-content information relating to Internet communications was simply unprotected by Federal statutory law. Content information clearly protected by the Wiretap Act—that was made clear in 1986—but non-content information left unclear under the Electronic Communications Privacy Act and not clarified until the PATRIOT Act.

Section 216 of the PATRIOT Act did make clear that that law applies to the Internet, an important change, I think, because it makes clear that, for example, the Government does need a court order to conduct non-content monitoring. The possibility that was present before the PATRIOT Act was that actually the lack of clarity as to whether the law applied could have made it such that no court order was necessary for the Government to, for example, install Carnivore in the Internet. This law actually struck a balance, which I think is on the road to the proper balance, but only part of the way, toward making a better balance on Internet communications.

In particular, I would say—agree with Mr. Dempsey that a higher standard for the pen register law is probably a good idea—something like the specific and articulable facts standard which governs stored communications, stored non-content communications. That's found in 18 USC 2703(d)—I think a sensible move to raise the threshold in that law.

I would also say, on the question of section 215, the controversial law applying to—that people are worried applies to libraries, sort of an equivalent to a subpoena authority for terrorism investigations. How worrisome that law is really depends on what your point of reference is. So for example the Government says, well, the point of reference should be criminal authorities and in particular the subpoena authority, grand jury subpoena, which has traditionally been used to obtain records at libraries. And if you look at section 215 with that as your frame of reference, section 215 is not all that different, sort of a national security version of this traditional grand jury authority.

However, you could look at it from another perspective, sort of ignore the fact that there's this traditional existing subpoena authority, and say in the abstract, this is a pretty worrisome law and in fact the difficulty is that the subpoena rules don't regulate privacy enough and that we need to raise both standards rather than move to the lower standard for both.

I think the answer is in clarification of the existing standard. To find a slightly better balance, I agree—somewhere in between, I would say, between these two standards, and that's the right approach.

Thank you.

[The prepared statement of Mr. Kerr follows:]

PREPARED STATEMENT OF ORIN S. KERR

Mr. Chairman and members of the Subcommittee, my name is Orin S. Kerr, and I am an Associate Professor at George Washington University Law School. I am grateful for the opportunity to appear before you today to discuss Internet surveillance law and the effect of the USA Patriot Act.

My testimony will focus on the controversial pen register amendments to the Patriot Act, found in Section 216 of the Act. As you know, these amendments have received a great deal of criticism. Critics have claimed that the amendments gave the government unprecedented powers to wiretap the Internet. I believe that these criticisms are misplaced. They are based on a misunderstanding of how the complex laws governing Internet surveillance interact with each other. When properly understood, the Patriot Act's provisions applying the pen register law to the Internet appear instead as an important first step toward modernizing the surveillance laws and protecting privacy in the Internet age. The pen register amendments to the Patriot Act are not so much part of the problem as they are an initial step toward a solution that will best balance the protection of privacy and the needs of law enforcement. In my testimony this afternoon, I will explain why I believe this is true. I will then suggest two additional steps that I believe Congress should take to develop this area of law in the future.

Before I begin, let me note that my testimony this afternoon is a streamlined version of an argument I made in a recent law review article. Those wishing to read more can look at the full article, "Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't." The article appears in the Winter 2003 issue of the *Northwestern University Law Review*, and it covers the pen register laws, the use of Carnivore, and the new computer trespasser exception to the Wiretap Act. A .pdf copy of the article can be downloaded for free from the Internet at this address: *http://papers.ssrn.com/sol3/papers.cfm?abstract—id=317501*.

To begin understanding the effect of the Patriot Act's pen register amendments, it helps to start with some history. The surveillance laws that apply to the Internet were originally designed to apply to the telephone network. Telephone network surveillance is governed by two complementary laws: the Wiretap Act, enacted in 1968 and codified at 18 U.S.C. §§ 2510–22; and the Pen Register Statute, enacted in 1986 and codified at 18 U.S.C. §§ 3121–27. These two laws govern real-time surveillance of the telephone network in criminal investigations. The laws coexist because they cover different things: the Wiretap Act protects the "contents" of communications with a very high degree of privacy protection, and the Pen Register statute protects non-content addressing information with a lesser degree of privacy protection. This bifurcation between contents and non-content addressing information is consistent with and follows from the Supreme Court's cases interpreting how the Fourth Amendment applies to the telephone network. In *Berger* v. *New York*, 388 U.S. 41 (1967), the Supreme Court held that the Fourth Amendment protected the contents of telephone calls, whereas in *Smith* v. *Maryland*, 442 U.S. 745 (1979), the Supreme Court held that the Fourth Amendment does not protect non-content information relating to telephone calls such as might be collected by a pen register device, which was an early machine used to record the numbers dialed from a telephone.

The line between the Wiretap Act and the Pen Register statute is easy to understand for a traditional telephone call. If I place a phone call, the actual conversation between the person I call and myself are the "contents" of the call. If the government wishes to listen in on the call, the privacy protections of the Wiretap Act prohibit the government from doing so unless the government first obtains a Wiretap Order, which is a type of "super" search warrant. In contrast, information about the call such as my phone number, the time I called, the duration of the call, and the number I dialed is the non-content addressing information about the call. This information is protected by the Pen Register statute but not the Wiretap Act. If the government wishes to have the phone company record this information and disclose it to the government, the privacy protections of the Pen Register statute prohibit this unless the government first obtains a pen register order. A pen register order is a "relevance" court order; the government can obtain such an order if the information to be collected is relevant to an ongoing criminal investigation. The basic rule is that the lesser privacy protections of the Pen Register statute apply to non-content information, and the greater privacy protections of the Wiretap Act apply to content information.

Now let's turn from the telephone network to the Internet. In 1986, Congress enacted the Electronic Communications Privacy Act, also known as "ECPA." ECPA established that the Wiretap Act that protects the contents of telephone calls also protects the contents of Internet communications. ECPA also created a new privacy law known as the Stored Communications Act, codified at 18 U.S.C. §§ 2701–11, which

created statutory privacy protection for stored Internet communications such as stored e-mails. However, ECPA left a very important question unclear: what privacy protection if any applied to real-time surveillance of non-content addressing information for Internet communications? What law governs the real-time surveillance of Internet packet headers or e-mail headers—non-content addressing information that is the Internet equivalent of the outside envelope of a postal letter or the addressing information for a telephone call? The Pen Register statute that already protected equivalent information for telephone calls provided the obvious source of privacy protection, but its scope was unclear. As enacted in 1986, parts of the Pen Register statute appeared to apply broadly to protect both telephone and Internet communications. However, other parts of the statute seemed narrowly drafted to apply only to the telephone. These mixed signals left the scope of the Pen Register statute unclear. The text of the 1986 Act simply failed to answer whether the Pen Register statute protected the privacy of non-content Internet communications in the same way it protected the privacy of non-content telephone communications.

The uncertain scope of the Pen Register statute created a complicated situation for law enforcement before the enactment of the Patriot Act. The applicable law looked quite different depending on whether one assumed that the Pen Register law applied to the Internet. If the Pen Register statute did apply to the Internet, then the law prohibited the government from monitoring non-content information on the Internet without a pen register court order. It also made it a crime for private parties or foreign governments to conduct such surveillance. At the same time, the law would then authorize the government to conduct non-content surveillance (or order an Internet service provider to conduct such surveillance on the government's behalf) by obtaining a pen register order. If the Pen Register law did not protect the privacy of Internet communications, however, then no privacy law at all protected non-content information of Internet communications in transit. The government would be able to install Internet wiretapping devices such as "Carnivore" without any court order or any judicial review so long as the device did not collect any contents and was therefore exempt from the Wiretap Act. Any private citizen or foreign government would have been able to do the same. At the same time, the law would have left unclear what authority the government would be able to use to compel an Internet service provider to conduct such surveillance on the government's behalf.

In the period before the Patriot Act, the Department of Justice concluded that on balance the better argument was that the Pen Register statute did apply to the Internet. In other words, DOJ concluded that the law protected the privacy of Internet communications and required the government to obtain a court order before it could conduct real-time surveillance of non-content information on-line. Federal prosecutors routinely obtained pen register orders from magistrate judges in Internet crime investigations. While magistrate judges occasionally expressed initial concern over whether the Pen Register statute in fact applied to the Internet, every federal magistrate judge except one concluded that the statute did apply to the Internet and approved the government's application for the court order. The one magistrate judge who disagreed was located in San Jose, California. In an unpublished order in November 2000, this particular judge denied the government's ex parte application for a pen register order on the ground that the Pen Register statute did not apply to the Internet, but rather applied only to the telephone network.

Section 216 of the Patriot Act clarified that the Pen Register statute did in fact protect the privacy of Internet communications. It replaced the telephone-specific language from the 1986 Act with broader, technology-neutral language: the new version of the Pen Register statute protects any real-time non-content "dialing, routing addressing, or signaling information" relating to either telephone or Internet communications. In practice, this amendment maintained the status quo: it permitted the Justice Department to continue its pre-Patriot Act procedures. How much the change altered existing law in a formal sense depends upon whether you conclude that the Pen Register law applied to the Internet before the Patriot Act. If you believe that the Pen Register law did already apply, then the amendment merely clarified existing law. If you believe that it did not, the amendment extended the privacy protection of the Pen Register statute to the Internet.

I believe this amendment was a positive step forward that would have won widespread support if it had been better understood at the time of the Patriot Act's passage. The amendment expanded the scope of a privacy law, making sure that the government needed a court order where before it was possible that no court order was necessary. Why did this provision trigger such controversy? One reason is that many commentators incorrectly believed that the Pen Register amendments lessened the protections of the companion Wiretap Act. Many commentators wrongly assumed that before the Patriot Act, the Wiretap Act had protected both contents and non-content information. Based on that incorrect assumption, they concluded that

the Pen Register amendments lessened privacy protections by moving the protection of non-content information from the high privacy protections of the Wiretap Act to the lower protections of the Pen Register statute. This led to widely-reported claims that the Pen Register amendments gave the government unprecedented new powers to wiretap the Internet without a probable cause search warrant.

The premise is mistaken, however. The Wiretap Act protects only the contents of communications; it does not protect non-content information. This was true both before and after the Patriot Act. The Patriot Act did not change the scope of the Wiretap Act's protection of contents; it left unchanged the statutory definition of "contents" in 18 U.S.C. § 2510(8) that has existed since 1986. To the extent the pen register amendment of the Patriot Act changed the law at all, it increased the scope of privacy protections by making sure that non-content information was not left unprotected by federal privacy law. This did empower the government to obtain court orders in Internet crime investigations under the low pen register standard: as is always the case with laws regulating surveillance, the power to seek a court order to conduct the surveillance is an exception to the law that applies when the law regulates the surveillance. But the pen register amendment did not lessen the protections of the Wiretap Act. Instead it clarified that the same rules apply to the Internet that have traditionally applied to the telephone.

I stated at the beginning of my testimony that the pen register amendments of the Patriot Act were an important first step toward modernizing the Internet surveillance laws and protecting privacy. This raises the question, what steps remain? I think there are two areas that should demand Congress's attention in the future.

First, Congress should clarify the line between "contents" protected by the Wiretap Act and "dialing, routing, addressing, and signaling information" protected by the Pen Register statute. Today we know that human-to-human communications such as the body and the subject lines of e-mails count as "contents." We also know that computer-to-computer communications such as Internet Protocol packet headers count as "dialing, routing, addressing, and signaling information." However, we don't know how human-to-computer communications are treated under current law. Just two weeks ago, one court suggested that search terms entered into Internet search engines are contents protected by the Wiretap Act. *See* In re Pharmatrak, Inc. Privacy Litigation,—F.3d—, 2003 WL 21038761 (1st Cir. May 9, 2003). Three years ago, another court indicated that passwords entered into computers are also contents protected by the Wiretap Act. *See United States Telecom Ass'n* v. *FCC*, 227 F.3d 450, 462 (D.C. Cir. 2000). However, the absence of a statutory suppression remedy in the Internet surveillance laws means that these decisions appear only sporadically in unusual civil contexts, and tend to have uncertain scope. Congress should either add a statutory suppression remedy that will have the effect of empowering the courts to clarify the line between the two statutes in criminal cases, or should take steps to clarify that line itself.

Second, I believe that Congress should raise the standard that the government needs to satisfy to obtain a pen register court order. First, the factual threshold should be raised from mere relevance to "specific and articulable facts," matching the protection that exists under current law for stored non-content records. *See* 18 U.S.C. § 2703(d). Second, the current certification standard should be replaced with judicial review. Current law states that the government lawyer applying for a pen register order must certify that the factual threshold has been satisfied, and requires the magistrate judge to grant the application if the certification has been made. The law should be changed so that magistrate judges evaluate whether the government's application satisfies the factual showing. Again, this matches the protection that exists under current law for stored non-content records. The added judicial review will provide the public a greater assurance that the law is not being abused, whether in the telephone context or the Internet context. At the same time, based on my experience as a federal prosecutor I believe that the slightly higher threshold will not create a substantial burden for law enforcement.

Let me conclude by offering a few thoughts on the big picture. Today the law of Internet surveillance in criminal investigations remains governed primarily by the Electronic Communications Privacy Act of 1986. Congress has amended this law several times since 1986, including when it passed the USA Patriot Act, but the basic framework of the 1986 law remains in place. The 1986 Act was a remarkable achievement for its day: it protected the privacy of Internet communications long before most Americans had even heard of the Internet. Even today, the law remains surprisingly workable and effective. The 1986 Act left many questions unresolved, however. The fast pace of technological change raises the bar as well; developments such as the World Wide Web require us to fit new technologies into old laws. As a result, the Internet surveillance laws demand constant legislative attention both

to address existing problems latent in the 1986 statutory scheme and to address new difficulties raised by technological change.

Fortunately, the provisions of the USA Patriot Act that relate to Internet surveillance in criminal investigations are much more balanced than many have feared. Much of the media coverage surrounding provisions such as the pen register amendments failed to appreciate the complex inner workings of the law, and as a result tended to misrepresent the effect of the Patriot Act in ways that made the Patriot Act seem more of a departure from existing law than it actually was. On reflection, today we can see that changes such as the pen register amendment did not substantially shift the balance between privacy and security. Rather, the law updated a 1986 privacy law and clarified that the same privacy protection that applies to the telephone also applies to the Internet. Much work remains to be done; the statutory laws that regulate Internet surveillance will surely keep Congress busy for years to come. However, the pen register amendments of the USA Patriot are best understood as part of a necessary response to preexisting ambiguities and technological change. They are consistent with rather than a departure from Congress's historical efforts to create rules that effectively balance privacy and security in new technologies.

Mr. CHABOT. Thank you, Professor. And our final witness this afternoon will be Mr. Rosenzweig.

STATEMENT OF PAUL ROSENZWEIG, SENIOR RESEARCH FELLOW, THE HERITAGE FOUNDATION

Mr. ROSENZWEIG. Thank you, Mr. Chairman. And thank you very much for the opportunity to be here. It's pleasing to hear one's words quoted back at one, although I confess, Mr. Nadler, that if I go back and tell them that you've quoted me, they're going to wonder what's up back at the Heritage Foundation as well. But——

Mr. NADLER. You never know what conspiracies are afoot on this Committee.

Mr. ROSENZWEIG. But what I think that that demonstrates, actually, is that this is an issue where those who are traditionally skeptical of Big Government because of its ability to invade people's social privacy, and those who are—who come from my tradition of skepticism about Big Government as an engine for economic and—change, tend to find a little bit more common ground.

Taking seriously the Committee's question posed in the title of the hearing about the Fourth Amendment—that is, whether or not the Fourth Amendment places any limits on what the Government can do—I think the candid answer is "not really," under the current state of Fourth Amendment jurisprudence. The Court has said since 1967 that information one voluntarily exposes to public display, it doesn't come within the scope of what is deemed a search and therefore subject to the Fourth Amendment.

Another way of thinking about it is a rhetorical question I sometimes ask, which is, "What is the single greatest constitutional violation of the Fourth Amendment that has occurred since September 11?" And in my judgment, the answer probably is the stopping of every car on the highway without cause or suspicion in our vain efforts, through that method, to find the snipers who plagued Washington, DC, last summer—plainly an unconstitutional act under *Indianapolis* v. *Edmonds* and other Supreme Court decisions, but one that almost nobody seemed to actually complain about at the time.

By contrast, the constitutional limitations on the access to non-information—for example, pen registers and addressing informa-

tion on the Internet—has, at least since the mid-1970's, been clearly—there's clearly been no protection at all. Thus we are left with a constitutional regime where the only limits on Government activity, Executive Branch activity must stem from the positive law enacted by this Congress, this—and originating generally in this Committee, i.e., the PATRIOT Act, which is why we are focused principally today on the provisions of the PATRIOT Act and the specific words therein, because they are supplements and in addition to what is, at least in the current regime, very minimal constitutional protections.

Turning, then, to what this Committee has done—or I'll address an area where the Committee has done very little, the recent FBI change in investigative guidelines relating to the FBI's ability to enter into public places and access public information on the Internet.

As I said, right now, since that information is exposed to the public by the original data holder or the attendees at the public meetings, there's very little the Constitution has to say. There's also very, very little that the PATRIOT Act has to say about the lawfulness of those activities. They are guided almost exclusively by the Attorney General's guidelines and past historical practice. In some instances, the courts have stepped in to regulate excessive uses of this investigative authority as trenching, perhaps, upon First Amendment concerns; that is, where the police use the authority, law enforcement uses the authority to enter into public places for the purposes of gaining information about an association, its members, or its exercise of First Amendment activity in a way that is intended to impinge upon that. But right now, there is nothing, at least—let me amend—very little that mandates the Attorney General's guidelines presently in place be used and mandates that these be the particular ones that are chosen.

For my part, I think ultimately the question that this Committee has to face in addressing the guidelines and, frankly, in addressing all of these concerns, is whether or not we should maintain a high set of standards knowing that in doing so we may miss some investigative opportunities, important investigative opportunities that might protect the American public; or lower those standards, accepting that there may be some abuse, and hope and expect that congressional oversight, of the form that my colleagues on the panel have already talked about, will protect those. As a strong backer of congressional oversight and a believer in it, I hope that the latter is sufficient.

And I see my time's expired, so I will be happy to get into more detail.

[The prepared statement of Mr. Rosenzweig follows:]

PREPARED STATEMENT OF PAUL ROSENZWEIG

Good afternoon Mr. Chairman and Members of the Subcommittee. Thank you for the opportunity to testify before you today on the challenge of maintaining the balance between security and constitutionally protected freedoms inherent in responding to the threat of terror, especially in the government investigations and data mining.

For the record, I am a Senior Legal Research Fellow in the Center for Legal and Judicial Studies at The Heritage Foundation,[1] a nonpartisan research and educational organization. I am also an Adjunct Professor of Law at George Mason University where I teach Criminal Procedure and an advanced seminar on White Collar and Corporate Crime. I am a graduate of the University of Chicago Law School and a former law clerk to Judge Anderson of the U.S. Court of Appeals for the Eleventh Circuit. For much of the past 15 years I have served as a prosecutor in the Department of Justice and elsewhere, prosecuting white-collar offenses. During the two years immediately prior to joining The Heritage Foundation, I was in private practice representing principally white-collar criminal defendants. I have been a Senior Fellow at The Heritage Foundation since April 2002.

My perspective on this matter, then, is that of a lawyer and a prosecutor with a law enforcement background, not that of technologist or an intelligence officer/analyst. I should hasten to add that much of my testimony today is based upon a series of papers I have written on various aspects of this topic and testimony I have given before other bodies in Congress, all of which are available at The Heritage Foundation website (www.heritage.org). For any who might have read this earlier work, I apologize for the familiarity that will attend this testimony. Repeating myself does have the virtue of maintaining consistency—I can only hope that any familiarity with my earlier work on the subject does not breed contempt.

It is a commonplace for those called to testify before Congress to commend the Representatives or Senators before whom they appear for their wisdom in recognizing the importance of whatever topic is to be discussed—so much so that the platitude is often disregarded as mere puffery. Today, however, when I commend this Subcommittee for its attention to the topic at hand—the difficulty of both protecting individual liberty and enabling our intelligence and law enforcement organizations to combat terror—it is no puffery, but rather a heartfelt view. I have said often since September 11 that the civil liberty/national security question is the single most significant domestic legal issue facing America today, bar none. And, as is reflected in my testimony today, in my judgment one of the most important components of a responsible governmental policy addressing this difficult question will be the sustained, thoughtful, non-partisan attention of America's elected leaders in Congress. Nothing is more likely, in my judgment, to allow America to find the appropriate balance than your engagement in this issue.

What I would like to do today is assist your consideration of this question by sharing with you some general legal analysis on the scope of the Fourth Amendment as it might apply in this context. I then offer some theoretical principles that you might consider in structuring your thinking. Finally, in an effort to avoid being too theoretical, I'd like to apply those principles to the concrete issues of data mining in the Total Information Awareness (TIA) program and the revised FBI investigative guidelines.

But let me first give you a short, pithy answer to the question posed by the title of today's hearing: Where and when can the government go to prevent terrorist attacks? The short answer is: "As a matter of constitutional law, virtually anywhere that any other member of the public can go." The more difficult and interesting question is how best should those efforts be regulated as a matter of public policy so as to increase our ability to combat terror while minimizing any infringement on American liberty interests.

FOURTH AMENDMENT PRINCIPLES

Under settled modern Fourth Amendment jurisprudence, law enforcement may secure without a warrant (through a subpoena) an individual's bank records, telephone toll records, and credit card records, to name just three of many sources of data. Other information in government databases (e.g. arrest records, entries to and exits from the country, and driver's licenses) may be accessed directly without even the need for a subpoena.

---

[1] The Heritage Foundation is a public policy, research, and educational organization operating under Section 501(c)(3). It is privately supported, and receives no funds from any government at any level, nor does it perform any government or other contract work. The Heritage Foundation is the most broadly supported think tank in the United States. During 2002, it had more than 200,000 individual, foundation, and corporate supporters representing every state in the U.S. Its 2002 contributions came from the following sources: Individuals (61%); Foundations (27%); Corporations (7%); Investment Income (1%); and Publication Sales and Other (3%). Members of The Heritage Foundation staff testify as individuals discussing their own independent research. The views expressed are their own and do not reflect an institutional position for The Heritage Foundation or its board of trustees.

In 1967, the Supreme Court said that the Fourth Amendment protects only those things in which someone has a "reasonable expectation of privacy" and, concurrently, that anything one exposes to the public (i.e., places in public view or gives to others outside of his own personal domain) is not something in which he has a "reasonable" expectation of privacy—that is, a legally enforceable right to prohibit others from accessing or using what one has exposed. So, for example, federal agents need no warrant, no subpoena, and no court authorization to:

- have a cooperating witness tape a conversation with a third party (because the third party has exposed his words to the public);
- attach a beeper to someone's car to track it (because the car's movements are exposed to the public);
- fly a helicopter over a house to see what can be seen; or
- search someone's garbage.

Thus, an individual's banking activity, credit card purchases, flight itineraries, and charitable donations are information that the government may access because the individual has voluntarily provided it to a third-party. According to the Supreme Court, no one has any constitutionally based enforceable expectation of privacy in them. The individual who is the original source of this information cannot complain when another entity gives it to the government. Some thoughtful scholars have criticized this line of cases, but it has been fairly well settled for decades.

Congress, of course, may augment the protections that the Constitution provides and it has with respect to certain information. There are privacy laws restricting the dissemination of data held by banks, credit companies, and the like. But in almost all of these laws (the Census being a notable exception), privacy protections are good only as against other private parties; they yield to criminal, national security, and foreign intelligence investigations. Thus, the extent of privacy protection is mostly a creature of legislation, not constitutional provisions.

One important caveat or note should be made here—in the foregoing discussion I have spoken principally of the restrictions that apply to domestic law enforcement officials. Important additional restrictions continue to exist on the authority of foreign intelligence agencies to conduct surveillance or examine the conduct of American citizens. Conversely, however, the courts have recognized that in the national security context the requirements of the Fourth Amendment apply somewhat differently than they do in the context of domestic law enforcement. Since the issues before the Subcommittee today are, as I understand it, principally focused on domestic law enforcement activity—potential domestic uses of TIA and the FBI's investigative guidelines—I will simply note the distinction here and then, for purposes of discussion, allude to it no further.

OVERARCHING PRINCIPLES

Since I conclude that, for the most part, limitations on law enforcement are likely to be the product of policy rather than constitutional law, let me next share with you some general thoughts about how cautious, yet effective governmental action can, in my view, be implemented. Fundamental legal principles and conceptions of American government should guide the configuration of our intelligence and law enforcement efforts rather than the reverse. The precise contours of any rules relating to the use of any new technology or new program will depend, ultimately, on exactly what the new program is capable of or intended to accomplish—the more powerful the system or program, the greater the safeguards necessary. As a consequence, the concerns of civil libertarian critics should be fully voiced and considered while any research program is underway.

In general, unlike civil libertarian skeptics, I believe that new intelligence and law enforcement information gathering and information analytical systems can (and should) be constructed in a manner that fosters both civil liberty and public safety. We should not say that the risks of such systems are so great that any effort to construct them should be dispensed with.

Rather in my view, the proper course is to ensure that certain overarching principles animate and control the architecture of any new program and provide guidelines that will govern implementation of the program in the domestic environment.

The Common Defense—Let me make one important preliminary point: Most of the debate over new intelligence systems focuses on perceived intrusions on civil liberties, but Americans should keep in mind that the Constitution weighs heavily on both sides of the debate over national security and civil liberties. The President and Congressional policymakers must respect and defend the individual civil liberties guaranteed in the Constitution when they act, but there is also no doubt that they cannot fail to act when we face a serious threat from a foreign enemy.

The Preamble to the Constitution acknowledges that the United States government was established in part to provide for the common defense. The war powers were granted to Congress and the President with the solemn expectation that they would be used. Congress was also granted the power to "punish . . . Offenses against the Law of Nations," which include the international law of war, or terrorism. In addition, serving as chief executive and commander in chief, the President also has the duty to "take Care that the Laws be faithfully executed," including vigorously enforcing the national security and immigration laws.

Thus, as we assess questions of civil liberty I think it important that we not lose sight of the underlying end of government—personal and national security. I do not think that the balance is a zero-sum game, by any means. But it is vital that we not disregard the significant factors weighing on both sides of the scales.

Civil Liberty—Of course, just because the Congress and the President have a constitutional obligation to act forcefully to safeguard Americans against attacks by foreign powers does not mean that every means by which they might attempt to act is necessarily prudent or within their power. Core American principles require that any new counter-terrorism technology deployed domestically) should be developed only within the following bounds:

- No fundamental liberty guaranteed by the Constitution can be breached or infringed upon.
- Any increased intrusion on American privacy interests must be justified through an understanding of the particular nature, significance, and severity of the threat being addressed by the program. The less significant the threat, the less justified the intrusion.
- Any new intrusion must be justified by a demonstration of its effectiveness in diminishing the threat. If the new system works poorly by, for example, creating a large number of false positives, it is suspect. Conversely, if there is a close "fit" between the technology and the threat (that is, for example, if it is accurate and useful in predicting or thwarting terror), the technology should be more willingly embraced.
- The full extent and nature of the intrusion worked by the system must be understood and appropriately limited. Not all intrusions are justified simply because they are effective. Strip searches at airports would prevent people from boarding planes with weapons, but at too high a cost.
- Whatever the justification for the intrusion, if there are less intrusive means of achieving the same end at a reasonably comparable cost, the less intrusive means ought to be preferred. There is no reason to erode Americans' privacy when equivalent results can be achieved without doing so.
- Any new system developed and implemented must be designed to be tolerable in the long term. The war against terror, uniquely, is one with no immediately foreseeable end. Thus, excessive intrusions may not be justified as emergency measures that will lapse upon the termination of hostilities. Policymakers must be restrained in their actions; Americans might have to live with their consequences for a long time.

From these general principles can be derived certain other more concrete conclusions regarding the development and construction of any new technology:

- No new system should alter or contravene existing legal restrictions on the government's ability to access data about private individuals. Any new system should mirror and implement existing legal limitations on domestic or foreign activity, depending upon its sphere of operation.
- Similarly, no new system should alter or contravene existing operational system limitations. Development of new technology is not a basis for authorizing new government powers or new government capabilities. Any such expansion should be independently justified.
- No new system that materially affects citizens' privacy should be developed without specific authorization by the American people's representatives in Congress and without provisions for their oversight of the operation of the system.
- Any new system should be, to the maximum extent practical, tamper-proof. To the extent the prevention of abuse is impossible, any new system should have built-in safeguards to ensure that abuse is both evident and traceable.
- Similarly, any new system should, to the maximum extent practical, be developed in a manner that incorporates technological improvements in the protection of American civil liberties.

- Finally, no new system should be implemented without the full panoply of protections against its abuse. As James Madison told the Virginia ratifying convention, "There are more instances of the abridgment of the freedom of the people by gradual and silent encroachments of those in power than by violent and sudden usurpations."

"DATA MINING"—TOTAL INFORMATION AWARENESS TODAY

To that end, let me first discuss the concept of data mining and more particularly the Total Information Awareness program ("TIA")—a program that has been widely misunderstood. [For more detail on the program I refer you to a paper I co-authored with my Heritage colleague, Michael Scardaville—"The Need to Protect Civil Liberties While Combating Terrorism: Legal Principles and the Total Information Awareness Program," The Heritage Foundation, Legal Memorandum No. 6 (February 2003).]

DATA ANALYSIS

First, and foremost, I think that much of the public criticism has obscured the fact that TIA is really not a single program. Virtually all of the attention has focused on the data mining aspects of the research program—but far more of the research effort is being devoted to providing tools for enhanced data analysis. In other words, TIA is not, as I understand it, about bypassing existing legal restrictions and providing governmental agencies with access to new and different domestic information sources. Rather, it is about providing better tools to enable intelligence analysts to more effectively and efficiently analyze the vast pool of data already at their disposal—in other words to make our analysts better analysts. These tools include, for example, a virtual private network linking existing counter-terrorism intelligence agencies. It would also include, for example, research into a machine translation capability to automatically render Arabic into English. While these developments certainly pose some threat to civil liberty because any enhancement of governmental capability is inherently such a threat, they are categorically different than the data mining techniques that most concern civil libertarians. The threat to civil liberty is significantly less and the potential gain from their development is substantial.

Thus, my first concrete recommendation to you is to not paint with too broad a brush—the distinction between collection and analysis is a real and important one that, thus far, Congress has failed to adequately recognize. Earlier this year, Congress passed an amendment, the so-called Wyden amendment, which substantially restricts TIA development and deployment. That restriction applies broadly to all programs under development by DARPA. That's a mistake. The right answer is not for Congress to adopt a blanket prohibition. Rather, Congress should commit to doing the hard work of digging into the details of TIA and examining its operation against the background of existing laws and the existing terrorist threats at home and abroad.

We have already seen some of the unintended but pernicious effects of painting with such a broad brush. Recently at a forum conducted by the Center for Strategic Policy, DARPA officials discussed how the Wyden amendment had short-circuited plans to sign a Memorandum of Understanding (MOU) with the FBI. The FBI, as this Subcommittee knows, is substantially behind the technological curve and is busily engaged in updating its information technology capabilities. The MOU under consideration would have enabled the FBI to join in the counter-terrorism Virtual Private Network (VPN) being created by the TIA program. Again, the VPN is not a new data collection technology—it is a technology to enhance data analysis by allowing information sharing. Other counter-terrorism agencies with exclusively foreign focus are already part of the VPN—the CIA and DIA for example. Though the Department of Defense has not reached a final interpretation of the Wyden amendment, the lawyers at DoD were sufficiently concerned with its possible scope that they directed DARPA to not sign the MOU with the FBI. As a consequence one of our principal domestic counter-terrorism agencies is being excluded from a potentially valuable network of information sharing. Extrapolating from this unfortunate precedent, it is likely that the Wyden amendment will have the effect of further balkanizing our already unwieldy domestic counter-intelligence apparatus. The same law will probably be interpreted to prohibit the Department of Homeland Security from joining the network, as well as the counter-terrorism agencies of the various States.

In short, as Senator Shelby has written of TIA:

> The TIA approach thus has much to recommend it as a potential solution to the imperative of deep data-access and analyst empowerment within a 21st-century Intelligence Community. If pursued with care and determination, it has

the potential to break down the parochial agency information "stovepipes" and permit nearly pure all source analysis for the first time—yet without unmanageable security difficulties. If done right, moreover, TIA would be infinitely scalable: expandable to as many databases as our lawyers and policymakers deem to be appropriate.

TIA promises to be an enormously useful tool that can be applied to whatever data we feel comfortable permitting it to access. How broadly it will ultimately be used is a matter for policymakers to decide if and when the program bears fruit. It is worth emphasizing, however, that TIA would provide unprecedented value-added even if applied exclusively within the current Intelligence Community—as a means of finally providing analysts deep but controlled and accountable access to the databases of collection and analytical agencies alike. It would also be useful if applied to broader U.S. Government information holdings, subject to laws restricting the use of tax return information, census data, and other information. Ultimately, we might choose to permit TIA to work against some of the civilian "transactional space" in commercially-available databases that are already publicly and legally available today to marketers, credit card companies, criminals, and terrorists alike. The point for civil libertarians to remember is that policymakers can choose to restrict TIA's application however they see fit: it will be applied only against the data-streams that our policymakers and our laws permit.

Put more prosaically, it remains for this Congress to decide how widely the analytical tools to be provided by TIA are used—but it is imperative that Congress understand that the tools themselves are distinct from the databases to which they might have access.

DATA COLLECTION—STRUCTURAL LIMITATIONS

As for concerns that the use of new data collection technologies will intrude on civil liberties by affording the government access to new databases, I certainly share those concerns. The question then is how best to ensure that any domestic use of TIA (or, frankly, any other intelligence gathering program) does not unreasonably intrude on American domestic civil liberties. There are several operational principles that will effectively allow the use of TIA while not substantially diminishing American freedom. Amongst these are the following requirements:

Require congressional authorization. In light of the underlying concerns over the extent of government power, it is of paramount importance that there be formal congressional consideration and authorization of the TIA program, following a full public debate, before the system is deployed. Some of the proposed data-querying methods (for example, the possibility for access to non-government, private databases, which is discussed in the next section) would require congressional authorization in any event. But, more fundamentally, before any program like TIA—with both great potential utility and significant potential for abuse—is implemented, it ought to be affirmatively approved by the American people's representatives. Only through the legislative process can many of the restrictions and limitations suggested later in this testimony be implemented in an effective manner. The questions are of such significance that they should not be left to executive branch discretion alone.

Maintain stringent congressional oversight. In connection with the congressional authorization of TIA, Congress should also commit at the outset to a strict regime of oversight of the TIA program. This would include periodic reports on TIA's use once developed and implemented, frequent examination by the U.S. General Accounting Office, and, as necessary, public hearings on the use of TIA. Congressional oversight is precisely the sort of check on executive power that is necessary to insure that TIA-based programs are implemented in a manner consistent with the appropriate limitations and restrictions. Without effective oversight, these restrictions are mere parchment barriers. While potentially problematic, one can be hopeful that congressional oversight in this key area of national concern will be bipartisan, constructive, and thoughtful. Congress has an interest in preventing any dangerous encroachment on civil liberties by an executive who might misuse TIA.

My colleagues at The Heritage Foundation have written extensively on the need for reorganization of the congressional committee structure to meet the altered circumstances posed by the war on terrorism and the formation of the Department of Homeland Security. Oversight of any program developed by TIA would most appropriately be given either to the committee which, after reorganization, had principal responsibility for oversight of that Department or, if TIA is limited to foreign intelligence applications, to the two existing intelligence committees.

Construct TIA to permit review of its activities. To foster the requisite oversight and provide the American public with assurances that TIA is not being used

for inappropriate purposes, the TIA program must incorporate, as part of its basic structure, an audit trail system that keeps a complete and accurate record of activities conducted using the technology. To the maximum extent practical, the audit system should be tamper-proof. To the extent it cannot be made tamper-proof, it should be structured in a way that makes it evident whenever anyone has tampered with the audit system. Only by providing users, overseers, and critics with a concrete record of its activity can TIA-developed technology reassure all concerned that it is not being misused.

Limit the scope of activities for which queries of domestic non-government databases may be used. TIA is a technological response to the new, significant threat of terrorism at home and abroad. After September 11, no one can doubt that domestic law enforcement and foreign intelligence agencies face a new challenge that poses a qualitatively greater threat to the American public than any other criminal activity.

U.S. foreign counterintelligence efforts are responding to a new and different form of terrorism and espionage. It is appropriate, therefore, that the use of TIA to query non-government databases be limited to the exigent circumstances that caused it to be necessary. Technology being developed for TIA to build models, query and correlate data, and uncover potential terrorist activity should be used (whether for law enforcement or intelligence purposes) only to investigate terrorist, foreign intelligence, or national security activities, and the TIA technology should never be used for other criminal activity that does not rise to this level.

It is important to be especially wary of "mission creep," lest this new technology become a routine tool in domestic law enforcement. It should not be used to fight the improperly named "war on drugs," combat violent crime, or address other sundry problems. While certainly issues of significant concern, none of these are so grave or important as the war on terrorism. Given the bona fide fears of increased government power, any systems that might be derived from TIA should be used only for investigations where there is substantial reason to believe that terrorist-related activity is being perpetrated by organizations whose core purpose is domestic terrorism.

The legislation authorizing TIA should enact this limitation. Congress should, therefore, specify that use of the TIA system is limited to non-government data inquiries that are certified at a sufficiently high and responsible level of government to be necessary to accomplish the anti-terrorism objectives of the United States. Only if, for example, a Senate-confirmed officer of the Department of Justice, Homeland Security, FBI, or CIA (such as an Assistant Attorney General or the FBI Director) certifies the objectives of the query based upon a showing of need should one be made.

Limit access to the results of the search. A corollary to the need to limit authority to initiate an analysis using TIA is an equivalent necessity to limit access to the findings of any resulting analysis. It would be unacceptable, for example, for the data and analysis derived from a TIA query (or, for that matter, a CAPPS II query), and linked to an individual identity, to be available to every Transportation Security Administration screener at every airport. Assuredly, after high-level analysis substantiated the utility of the information, it could be used to create watch lists and other information that can be shared appropriately within the responsible agencies. Until that time, however, access to the results of a TIA search should be limited by the authorizing legislation to a narrow group of analysts and high-level officials in those intelligence, counterintelligence, and law enforcement agencies.

Distinguish between use of TIA in examining domestic and foreign activities. In practice, it will be possible to use whatever technology the TIA program develops to unearth terrorist activity or conduct counterintelligence activity both abroad and domestically. Existing law places significant restrictions on intelligence and law enforcement activity that addresses the conduct of American citizens or occurs on American soil. Conversely, fewer restrictions exist for the examination of the conduct of non-Americans abroad.

The development of TIA is not a basis for disturbing this balance and changing existing law. Thus, even if Congress ultimately chooses to prohibit the implementation of TIA for any domestic law enforcement purpose whatsoever (a decision that would be unwise), it would be a substantial expansion of existing restrictions on the collection of foreign intelligence data were it to extend that prohibition to use of the technology with respect to overseas databases containing information on non-citizens. At a minimum, in considering TIA, Congress should ensure that, consistent with existing law, any program developed under TIA will be used in an appropriate manner for foreign intelligence and counterintelligence purposes.

Impose civil and criminal penalties for abuse. Most important, all of these various prohibitions must be enforceable. Violations of whatever prohibitions Con-

gress enacts should be punishable by the executive branch through its administrative authority. Knowing and willful violations should be punishable as crimes. These forms of strong punishment are a necessary corollary of any TIA authorization.

In addition, Congress should enlist the third branch of government—the courts—to serve as a further check on potential abuse of TIA. As is detailed below, the courts will be involved in challenges to TIA information requests. To insure effective oversight of the use of TIA by the courts, Congress should also authorize a private right of civil action for injunctive relief, attorneys' fees, and (perhaps) monetary damages by individuals aggrieved by a violation of the restrictions Congress imposes.

Sunset the authorization. Any new law enforcement or intelligence system must withstand the test of time; it must be something that the American public can live with, since the end of the war on terrorism is not immediately in sight. Congress should be cautious, therefore, in implementing a new system of unlimited duration. It is far better for the initial authorization of TIA to expire after a fixed period of time so that Congress may evaluate the results of the research program, its costs (both public and private), and its long-term suitability for use in America. A sunset provision of five years would be ample time for Congress to gather concrete information on the program. With such information, Congress will be in a position to continue, modify, or terminate the program, as it deems appropriate.

DATA COLLECTION—LEGAL LIMITATIONS

As I noted earlier, the existing legal structure and the overarching principles that I see in American law lead to a singular legal recommendation for the structure and operation of TIA:

> *TIA should be implemented only in a manner that mirrors existing legal restrictions on the government's ability to access data about private individuals—nothing more and nothing less.*

This recommendation may be particularized in the following ways:

TIA should not have access to protected governmental databases. Most government databases (e.g., arrest records and driver's licenses) contain information about an individual that is accessible to the government and in which the individual has no reasonable expectation of privacy. Linking such information through TIA technology should not be subject to any greater restriction than that applied to its initial inclusion in the local, state, or federal government database from which the information is retrieved. By contrast, some existing governmental databases (like the Census database) cannot be used for purposes other than those for which they were created. Others (like the IRS database on taxpayer returns) can be accessed only with a special court order.

In authorizing the development of TIA technology, Congress should make it clear that information from existing government databases may be queried using TIA structured query programs only to the extent that the government already lawfully has access to the data. The creation of TIA-based networks should not be viewed as an excuse or opportunity to remove existing restrictions on the use of particularly sensitive individual data.

Information from private domestic databases should be accessed only after notice to the data holder. A similar limitation should also apply to queries made of private, non-government databases from which the government seeks information. Where predication for an investigation (whether criminal or foreign intelligence) exists, law enforcement or intelligence authorities should have the ability to secure data about an individual or pattern of conduct from private databases just as they do under current law.

Thus, with appropriate predication and/or court authorization (if the law requires), the government should be able to secure data from banks, credit card companies, and telephone companies about the conduct of specified individuals or about specified classes of transactions. But existing warrant and subpoena requirements should not be changed. Such data gathering should be done only at the "retail" level when a particularized basis for investigation exists.

More important, in each instance where data is sought from a private database, the holder of the data should be notified prior to securing the data and (as in the context of a subpoena today) have the capacity to interpose an objection to the data query to the same extent the law currently permits. The law today does not provide a mechanism by which such information requests may be made other than by subpoena. Thus, in authorizing a TIA-based investigative system, Congress should require that any aspects of TIA seeking data from private databases should operate in a manner similar to that in contemporary subpoena practice.

As this analysis makes evident, one should strongly oppose any effort to incorporate in TIA the ability to gather private database information at the "wholesale" level (e.g., all bank transactions processed by Citibank). One should also strongly oppose any TIA-based system that allows access to privately held data without notice to (and the opportunity to object by) the data holder. In short, the development of TIA technology and the war on terrorism is not a justification for the routine incorporation of all private data and information in a single government database.

TIA is not a justification for creating new government databases. Given the clear distinction that the law enacts between access to government and access to private, non-government databases, a further cautionary note is in order. In order to evade the legal strictures limiting access to information in private databases, the government might be tempted, in effect, to "institutionalize" the information it deems relevant by enacting new data-reporting requirements to capture in government databases information that now exists only in private databases to which access is less ready. The first such proposal may already have been made: that Americans flying abroad be required to provide their travel itineraries to the Transportation Security Administration upon their departure from America.

The expansion of existing government databases should be resisted except upon a showing of extraordinary need. The government already collects too much information about Americans on a day-to-day basis. While many government programs require the collection of such data to permit them to operate, one should not create databases where no program requiring their creation exists—otherwise, there is the risk of wholesale evasion of existing legal restrictions on the use of information in private databases. Initiatives such as the new itinerary-collection program should be evaluated independently to determine their necessity and utility.

There must be absolute protection for fundamental constitutionally protected activity. The gravest fear that most Americans have about TIA is that it might be used to transmit queries about and assemble dossiers of information on political opponents. One should not discount these fears as they rest on all-too-recent abuses of governmental power. If a system developed based on TIA technology is used to enable an effort to harass anti-war demonstrators or gather information on those who are politically opposed to the government's policies (as the FBI used its investigative powers to do in the 1960s and 1970s), such abuse should be terminated immediately.

This prospect is not, however, sufficient to warrant a categorical rejection of all of the benefits to the war on terrorism that TIA technology might provide. TIA can be developed without these abuses, and aspects of the technology under investigation in fact hold the promise of enhancing civil liberties. Still, it is imperative that any implementing legislation has concrete, verifiable safeguards against the misuses of TIA. These should include, for example, an absolute prohibition on accessing databases relating to support of political organizations that propagate ideas—even ones favorable to terrorist regimes—absent compelling evidence that the organizations also aid terrorist conspirators with monetary, organizational, and other support not protected by the First Amendment. There must be an absolute prohibition on accessing databases relating solely to political activity or protest.

TIA should build privacy protections into its architecture. Finally, it should be recognized that access to data is not necessarily equated with a loss of privacy. To be sure, it may in many instances amount to the same thing, but it need not. There is, for example, a sense in which the automated screening of personal data by computer enhances privacy: It reduces the arbitrariness or bias of human screening and insures that an individual's privacy will be disrupted by human intervention only in suspicious cases.

In addition, those developing TIA can be required to construct a system that initially disaggregates individual identifiers from pattern-based information. Only after the pattern is independently deemed to warrant further investigation should the individual identity be disclosed. So, for example, only after a query on the bulk purchase of the precursors of Ricin poison turned up a qualifying series of purchases linked to a single individual would the individual's name be disclosed to terrorism analysts.

Thus, everyone on both sides of the discussion should welcome one aspect of TIA, the Genisys Privacy Protection program. The Genisys program is developing filters and other protections to keep a person's identity separate from the data being evaluated for potential terrorist threats. In authorizing TIA, Congress should mandate that a trusted third party rather than an organization's database administrator control these protections.

FBI INVESTIGATIVE GUIDELINES

Let me turn now briefly to the new FBI investigative guidelines. Many of the principles I have applied to TIA, are equally relevant to any consideration of the recent changes in the FBI's investigative guidelines. I will not burden the record by repeating my analysis in its entirety here.

There are, however, aspects of the FBI's guidelines that suggest the need for heightened sensitivity to the potential for an infringement on protected constitutional liberties. As you will recognize from my testimony I have generally been supportive of the potential inherent in the development of the TIA system. In part, that reflects my belief in the benefits of technology. But it also reflects my conviction that existing Supreme Court precedent, dating back to the 1960s, accurately captures the scope of the Constitutional privacy protection embodied in the Fourth Amendment: The Constitution affords no additional protection to information that an individual has made available to other individuals or institutions. Privacy concerns relating to the further distribution of such information are matters of policy and legislative concern, not constitutional law. Similarly, the FBI guidelines raise no Fourth Amendment concerns, insofar as they authorize the FBI to collect publicly available information from public databases and/or public meetings.

Protecting Constitutional Liberties. Nonetheless the FBI guidelines do implicate potential threats to least two fundamental liberty interests guaranteed by the Constitution. Most obviously, the Supreme Court has long recognized a freedom of political association and the threat to that freedom posed by requiring organizations to identify their members. Second, many of the indicators that might be used to identify potential subjects of a terrorist investigation are also indicators that, in other circumstances, are potentially the products of protected First Amendment activity—in other words, though FBI investigative techniques are not intended to impinge upon free political speech or association, they may have the collateral effect of doing so.

Thus, there is a significant risk that a mal-administered system will impinge upon fundamental constitutional liberties. I am not, however, one to say that the risk of such impingement means abandonment of the program—especially not in light of the potentially disastrous consequences of another terrorist attack in the United States. I do, however, believe that some fairly stringent steps are necessary to provide the requisite safeguards for minimizing inadvertent or abusive infringements of civil liberty in the first instance and correcting them as expeditiously as possible. Those steps would include some or all of the following [many of which mirror recommendations I have already made with respect to TIA]:

- The FBI's use of these new investigative guidelines should be subject to extensive, continuous Congressional oversight. By this I do not mean the mere reporting of raw data and numbers—I mean that, at least as a spot check, Congress should examine individual, closed cases (if necessary using confidential procedures to maintain classified status) to assure itself that the investigative guidelines are not being misused. In other words, the database contemplated by the FBI guidelines should, under limited circumstances, be subject to congressional scrutiny;
- Authorization for "criminal intelligence" investigations under the FBI's guidelines should, in all circumstances, be in writing such that the FBI's internal system creates an "audit trail" for the authorization of investigations with potential First Amendment implications. Only through detailed record keeping can the use and/or abuse of investigative authority be reviewed;
- The FBI's new guidelines generally authorize the use of all lawful investigative techniques for both "general crimes" investigations and "criminal intelligence" investigations. There should be an especial hesitancy, however, in using the undisclosed participation of an undercover agent or cooperating private individual to examine the conduct of organizations that are exercising core First Amendment rights. When an organization is avowedly political in nature (giving that phrase the broadest definition reasonable) and has as its sole mission the advocacy of a viewpoint or belief, we should be especially leery of ascribing to that organization criminal intent, absent compelling evidence to that effect.
- There should, as well, be a hesitancy in visiting public places and events that are clearly intended to involve the exercise of core First Amendment rights, as the presence of official observers may chill expression. This is not to say that no such activity should ever be permitted—it is, however, to suggest the need for supervisory authorization and careful review before and after the steps are taken. Conversely, existing court consent decrees that expressly pro-

hibit all such activity (as is currently the case in New York City) should be revisited.

- No American should be the subject of a criminal investigation solely on the basis of his exercise of a Constitutionally protected right to dissent. An indication of threat sufficient to warrant investigation should always be based upon significant intelligence suggesting actual criminal or terrorist behavior.

Privacy. Though the FBI's guidelines authorize preliminary inquiries through the use of public information resources many Americans fear that these inquiries will result in the creation of personalized dossiers on dissenters. As it appears now, there are no explicit provisions in the guidelines for the destruction of records from preliminary inquiries that produce no evidence sufficient to warrant a full-scale investigation. One possible amendment to the guidelines that would ameliorate many privacy concerns would be an explicit provision providing for such destruction or, archiving with limited retrieval authority.

One other brief point should be made about privacy—in many ways the implementation of the FBI guidelines is not an unalloyed diminution of privacy. Rather it is the substitution of one privacy intrusion (into certain public spheres) for other privacy intrusions (into more private spheres, perhaps through other investigative means). It may also substitute for increased random investigations or the invidious use of racial, national origin, or religious classifications. Here one cannot make broad value judgments—each person weighs the utility of their own privacy by a different metric. But I do venture to say that for many Americans, the price of a little less public privacy might not be too great if it resulted in a little more personal privacy.

Mr. Chairman, thank you for the opportunity to testify before the Subcommittee. I look forward to answering any questions you might have.

Mr. CHABOT. Thank you very much. The Members of the Committee will now have an opportunity to ask questions of the panel for 5 minutes. I recognize myself for 5 minutes.

Mr. Dinh, I'll start with you. The USA PATRIOT Act requires the Government to maintain reports of the configuration of and duration of each time a program such as Carnivore is installed and any information which has been collected by the device. Under what circumstances would a court or a legislative body be able to review these reports?

Mr. DINH. Mr. Chairman, thank you very much. Section 216 of the USA PATRIOT Act does indeed require us to retain such information and to make it available to the issuing court within 30 days of the termination of the order in the ex parte review, for the court to review such information, including information relating to how it was used, what information was gathered by the device, and ultimately whether or not it was successful in gathering such information.

Mr. CHABOT. Okay, thank you. Can you tell us how many times, if at all, library records have been accessed under the new FISA standards and the USA PATRIOT Act, and if they have been so accessed, have the requests been confined to the library records of a specified person?

Mr. DINH. Mr. Chairman, section 215 of the USA PATRIOT Act requires the Department of Justice to submit semi-annual reports to this Committee and also to the House Intelligence Committee and the Senate counterparts on the number of times and the manner in which that section was used in total. We have made those reports. Unfortunately, they—because they occur in the context of a national-security investigation, that information is classified.

We have made, in light of the recent public information concerning visits to library, we have conducted an informal survey of the field offices relating to the—its visits to library. And I think the

result from this informal survey is that libraries have been contacted approximately 50 times based upon articulable suspicion or calls—voluntary calls from librarians regarding suspicious activities. Most if not all of these contacts that we have identified were made in the context of a criminal investigation and pursuant to voluntary disclosure or a grand-jury subpoena in that context.

Mr. CHABOT. It's my understanding that the first FBI guidelines and all subsequent guideline changes were adopted only after consultation with the House Judiciary Committee. What was the reason for breaking that tradition when the 2002 FBI guidelines were adopted?

Mr. DINH. Mr. Chairman, to be perfectly frank with you, I do not know the history of consultation or drafting of the 1976 Levi guidelines or the 1989 Thornburgh revisions or other revisions to the guidelines prior to this last round of revisions ordered by the Attorney General. I can say that after September 11, the Attorney General turned to a group of us, to me and the Office of Legal Policy in particular, and asked us to conduct a top-to-bottom review of all of our executive, administrative, and legislative authorities that are necessary to prosecute the global war against terrorism. Part of that review resulted in the USA PATRIOT Act, part of that review resulted in a number of administrative and regulatory changes, and part of that review resulted in the revisions to the guidelines and other guidelines. All of this was done very, very deliberately, but in a time-sensitive manner, and there was not consultation prior to the issuance of those guidelines.

However, at the conclusion of those revisions, we immediately consulted with this Committee and briefed and fully explained those guidelines. And we seek whatever wisdom you may give to us during this process.

Mr. CHABOT. Thank you. Does the FBI have in place an internal process in which track of how many agents have attended public events and, and of how many public events have been attended by agents?

Mr. DINH. Yes and no. In a first cut at the answer, we are interested in information relating to criminal and terrorist activity. That's why the Attorney General guidelines make clear that no information obtained from public visits shall be retained unless it relates to criminal and terrorist activities. That is the primary information which we track. And so in that sense, we do not track general visits as a matter of investigative activity, because we're interested in criminal investigations, not the ordinary activities of law-abiding citizens.

But there is an administrative control mechanism independent of investigative files. Each field office retains what we call a control file, which is an administrative file on how agents use their time. And in these control files, there are logged activities relating to their public visits. And those control files are accessible by headquarters or by supervising agents in order to determine the pattern and use of such visits.

Mr. CHABOT. Thank you. My time has expired. The gentleman from New York, Mr. Nadler, is recognized for 5 minutes.

Mr. NADLER. Thank you, Mr. Chairman.

Attorney General Dinh, I was interested to hear you say a few minutes ago that the number of times that libraries have been visited was classified information. The Department claims the mere fact as to whether the Department has used various authority granted in the PATRIOT Act is classified. The question is not when, where, how, or against whom. Is it your position that you can't even tell the Committee whether you have actually used the particular authority granted in the act?

You can't tell us—I mean, the libraries know whether they've been visited. How does it help the national security—why should it be classified how many libraries have been visited or even which—well, which—how many libraries have been visited? How do you suggest we evaluate the authority we have given you if you can't even tell us whether you've used those authority, how often you've used it?

Mr. DINH. That is a very fair question.

Mr. NADLER. Why should it be classified?

Mr. DINH. A very, very fair question. The total number of library visits is not classified. As I have said, we've done an informal survey and we've ascertained that approximately 50 library contacts have occurred in the past year. The precise use of FISA authorities, Foreign Intelligence Surveillance Act authorities, including the authority granted in section 215, is classified because they occurred in a national-security context.

Mr. NADLER. By "the precise," you mean against whom? I mean, which incidences?

Mr. DINH. No, even just the number, the number of FISAs used, the number——

Mr. NADLER. Why should the number be classified?

Mr. DINH. That is the determination of the classification Committee pursuant to——

Mr. NADLER. Well, that's nice, but why—what's the reason? Why should it be classified?

Mr. DINH. If I may—pursuant to Executive Order 12333 and the decision of the multi-agency task force——

Mr. NADLER. Yeah, but what's the reason?

Mr. DINH. The reason is fairly straightforward. The amount of activity as well as specific number of authorities used give an insight as to patterns of intelligence and terrorist activities that is known to the United States. If you will recall that FISA controls not only terrorists, but also spies. And so our ability to know what spy networks are there, what terrorist networks are there, the number of those networks——

Mr. NADLER. And so you're saying—excuse me. So what you're saying is that if you told us you've used the FISA authority 100 times or you've used it 1,000 times, that would tell some enemy something useful to them in terrorist activities?

Mr. DINH. Yes, sir. If, for example, in year one, in year one we said that we have an active number of FISAs that equals 100, and then in year two we say that that number has now changed to 200, that increase signifies an increased interest in our intelligence——

Mr. NADLER. Mr. Dempsey, could you comment on that, please?

Mr. DEMPSEY. Glad to, Mr. Nadler. The number of FISAs is actually published and known, and we watch how it goes up and down

from year to year. I think that the information that is published could be more detailed than that. Right now, there's a broad statement of the number of FISA applications that were granted.

I think in the case of the—going even down as specific as the number of times that section 215 has been used in a library—I happen to think that number's relatively small—I don't think that tells anybody anything. Because in fact, even in the case of terrorism investigations, the Government can be going in with subpoenas, criminal subpoenas. And so you—already you've got almost an apples-and-oranges question in terms of anybody trying to predict where the Government is or to try to evade Government surveillance. I think overall some of these numbers can be made publicly available. I think it would greatly help the subCommittee.

Mr. NADLER. Okay, thank you. Mr. Dinh, could you tell us what you consider to be the difference between content and not con—and non-content information in electronic communications? Do you have the technical means to segregate address lines from subject lines in an e-mail? How is this done, and how do you handle URL addresses?

Mr. DINH. Yes, yes, and that's a hard question. We consider non-content to be the To and From. The subject line is content. The—we have specified programs that are very precise in their parameters of what they will take and what they will not take. Congress recognized the existence of these programs by—when it enacted section 215, by requiring the Department to use the best available means in order to minimize non-content or excessive, or excessive take. With respect to URLs, the Deputy Attorney General has issued a memorandum, which has been provided to this Committee, on the use of post-cut-through intercepts in the analog world, and also content information in the digital world.

Mr. NADLER. I'd like Mr. Dempsey to comment on the same questions.

Mr. DEMPSEY. Well, I really think that the—we shouldn't overlook the main question, which is the inadequacy of the pen register standard right now. As Professor Kerr has referred to, that right now these orders are issued, that the statute says that the judge "shall" issues the order. The judge is required to issue the order if the Government asks for it. No factual showing, no——

Mr. NADLER. The judge has no discretion?

Mr. DEMPSEY. Absolutely no discretion.

Mr. NADLER. Does the Government have to show something to the judge to——

Mr. DEMPSEY. It has to show him a piece of paper signed by a prosecutor saying this is relevant to an investigation. The court cannot in fact ask, "Is it relevant?" If the Government——

Mr. NADLER. Should we amend that?

Mr. DEMPSEY. Well——

Mr. CHABOT. The gentleman's time has expired, but you can answer the question.

Mr. DEMPSEY. This Subcommittee and the full Committee in the 106th Congress approved legislation along the lines discussed by Professor Kerr that would require some minimal factual showing and some role for the judge, some actual finding by the judge that that information would be relevant to a criminal investigation.

Mr. CHABOT. The gentleman's time——

Mr. NADLER. That was superior to what you think is—you think that's superior to what's in the PATRIOT Act?

Mr. DEMPSEY. Absolutely.

Mr. NADLER. Thank you.

Mr. CHABOT. The gentleman's time has expired. The gentleman from Tennessee, Mr. Jenkins, is recognized for 5 minutes.

Mr. JENKINS. Thank you, Mr. Chairman.

Mr. Rosenzweig, you mentioned something that I've said many times in a little different way. But in my experience as a State legislator and here in the Congress, I've found that people who are separated greatly on the political spectrum, those people who call themselves very liberal and those people who call themselves very conservative——

Mr. CHABOT. Can you pull your mike, please, to——

Mr. JENKINS.—are much more likely to have greater accord when they have before them under consideration constitutional issues in general, and especially Fourth Amendment issues. And that's what, that's what you were saying. And I, I wonder if the other members of this panel also believe that to be true.

Mr. DINH. Yes, sir, the common bond that binds us is our U.S. Constitution and the procedures set forth thereunder.

Mr. JENKINS. And I have—Professor Kerr, do you believe that's the case?

Mr. KERR. I think there's, you know, widespread consensus that the Fourth Amendment is a vitally important constitutional protection. In terms of the politics, if that's more the question, there is—a rough cut could be that it tends sometimes to be the ends against the middle in these issues. But that's, of course, a pretty rough——

Mr. JENKINS. Well, this gives me a lot of confidence that this situation is not going to get out of hand, at least anywhere in the near future.

Another thing that nobody has mentioned here is the permanency of these provisions. Nobody has mentioned that with respect to, not all, but some of the these, there is a definite life to these provisions. It's, under the statute, what, 4 years for most? And does that not—is—does not, that not lessen the threat that some people fear? And any of you who would like to comment on that, let us know what you think about the sunset provisions, aspects of these provisions.

Mr. DEMPSEY. Congressman, I think that the sunset provision was in fact an important provision of the PATRIOT Act. I think that this hearing is part of the process of Congress deciding whether to reauthorize those provisions or whether to reauthorize them subject to better checks and balances.

I think, though, that a number of the things that we're talking about today and a number of the issues of concern to this Subcommittee do not arise under the PATRIOT Act and are not subject to the sunset. So the Subcommittee and the Congress is going to have to look at those as well. I think the FBI guidelines is one of those. I think the use of FISA, Foreign Intelligence Surveillance Act, information in criminal cases, that provision, I think, does not sunset, and that is an issue that will remain, that needs to be addressed. I think the pen register authority and what that should

be needs to be addressed. The use of data mining technology is taking place, really, outside of the PATRIOT Act, and standards and guidelines need to be established before that is implemented.

So the sunset, I think, is a symbol of Congress's responsibility. But mere up or down on the sunset doesn't, doesn't end the debate.

Mr. JENKINS. All right. Anybody else have a thought?

Mr. ROSENZWEIG. I'm a firm believer in the sunset provisions in this and other laws that relate to civil liberties, because to my mind, the fundamental check on executive excess which may or may not arise, but in preventing it, is the continued conscientious, nonpartisan engagement of Congress in oversight. And the sunset provisions are a way of ensuring that the institutional barriers that live in this institution that prevent activity sometime are overcome, in a sense binding yourselves to detailed, thoughtful oversight because of the impending sunset deadline. I think it's a great idea.

Mr. JENKINS. Anybody else? Mr. Chairman, that's all the questions I have.

Mr. CHABOT. Thank the gentleman. The gentleman's time has expired. The gentleman from Virginia, Mr. Scott, is recognized for 5 minutes.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. Dinh, is it the Administration's position that if the Secretary of Defense designates someone as a guilty foreign terrorist, that that person can be held indefinitely, no charges, no counsel, no judicial review? Is that the Administration's position?

Mr. DINH. Mr. Congressman, as you know, those cases, both in the 4th Circuit with Yaser Hamdi and the 2nd Circuit with Jose Padilla, are currently under litigation, so I'm somewhat limited in my ability to answer. I can say that in that litigation——

Mr. SCOTT. In a public document, did not the Administration take the position that after the Department of Defense designated somebody as a guilty terrorist, that the judicial branch ought to just butt out?

Mr. DINH. No, not exactly. The designation in Jose Padilla was made personally by the President of the United States as an unlawful enemy combattant, not necessarily guilty terrorist, but as an unlawful enemy combattant. That designation does in no way close the court house door to the combattant to challenge his detention. As a matter of fact, the courts are assessing——

Mr. SCOTT. Are you saying that the Administration took the position that the—Hamdi could in fact contest his designation in court, or was that what Judge Wilkinson made you do?

Mr. DINH. No, sir, what I'm saying is that the court house doors remain open in a habeas proceeding for Mr. Hamdi or Mr. Padilla in order to challenge his detention. And in the course of that habeas petition proceeding is how these issues are being resolved. It just so happens that the law and the facts——

Mr. SCOTT. Okay, let me be clear. It's your position that the Administration took the position that Mr. Hamdi had access to habeas corpus proceedings in court?

Mr. DINH. Let me put it this way. The President, has not suspended habeas corpus, as you—as we all know. And the court house door is open to all persons who——

Mr. SCOTT. And if I showed you a brief that said that the Administration position was that there was no habeas corpus available after the designation, you wouldn't know where that came from, would you?

Mr. DINH. Well, sir, there is a difference. There is a difference between the ability to present a habeas proceeding petition and whether or not that petition is entertainable by the court or has any merit on the law. The latter question, which I am addressing, is a matter that the court has issue. The former question is the one that I think, in specific answer to the question, we have not closed court house doors to present a habeas petition.

Mr. SCOTT. I'd ask unanimous consent that the staff obtain the Administration brief in the Hamdi case so that we can get the exact language. I think it would be inconsistent with what——

Mr. NADLER. Will the gentleman yield for a second?

Mr. SCOTT. I'll yield.

Mr. NADLER. The exact language was that once the President has designated someone an enemy—an unlawful combattant, the courts have no jurisdiction—no jurisdiction—to question that determination.

Mr. SCOTT. Well, reclaiming my time, I'd tell the gentleman from New York that's not what I just heard.

Mr. NADLER. I know it's not what you just heard. But it is the truth.

Mr. DINH. Let me be very, very clear. As I said, there are two separate questions here. One, whether or not the court house remains open to present a habeas petition; and two, whether or not that habeas petition, for jurisdictional or substantive reasons, has any merit.

Mr. SCOTT. Not merit, but—well——

Mr. DINH. In answer to your question——

Mr. SCOTT. Well, Mr. Hamdi was—well, we'll get the exact language and we'll see how the language of the brief comports with what you just said.

Is it—you mentioned the Levi guidelines. What is the change—has there been a change in FBI guidelines in terms of when you can start investigating—gathering information on people? The old guidelines used to require an underlying investigation before you started spying on people. Has that changed?

Mr. DINH. Under the old guidelines and in the new guidelines, the level of predication—initial checking out of leads, a preliminary investigation, or a full investigation—remains the same. What has changed is that the Attorney General, under Part VI of the new guidelines, adds this provision, and I quote: "For the purpose of detecting or preventing terrorist activities the FBI is authorized to visit any place and attend any event that is open to the public on the same terms and conditions as members of the public generally. No information obtained from such visits shall be retained unless it relates to potential criminal or terrorist activity."

Mr. SCOTT. Is that a change from what we had before?

Mr. DINH. That is a change from what we had before. Prior to that change, FBI agents were not able to stand on street corners and see whether crimes had been committed. They were not able to go on the Internet in order to search whether or not smallpox

is a threat. They had to do so only after they were picking up the rubble of the last terrorist attack.

Mr. SCOTT. Mr. Dempsey, if——

Mr. CHABOT. The gentleman's time has expired, but gentleman can ask his question.

Mr. SCOTT. I was going to ask if the—you have one of these database sweeps, who gets to look at the information? Thank you, Mr. Chairman.

Mr. DEMPSEY. Well, those are the rules that are not spelled out at all. Now, are you talking here about, as a follow-up to Mr. Dinh's comments about use of the Internet by FBI agents or by—are you talking about data mining issues?

Mr. SCOTT. Data mining.

Mr. DEMPSEY. Well, on the data mining issue, which is this use of the publicly available or commercial databases, we really don't know who gets to look at it, who they get to share it with, how long they can keep it, what the standards for accuracy are, who approves the search, who approves the sort of algorithm that is used to mine this data, who it can be disclosed to, how it can be characterized.

Mr. SCOTT. What about library books, library check-outs? Who gets to look at that information?

Mr. DEMPSEY. Well, once information is collected, particularly under the PATRIOT Act, it can be widely shared throughout the Government, almost without limitation.

Mr. CHABOT. The gentleman's time has expired. The gentleman from Iowa, Mr. King, is recognized for 5 minutes.

Mr. KING. Thank you, Mr. Chairman. Mr. Dinh, as I listened to you read that section, how it authorizes agents to go in any public gathering and gather such information as is available to the public, and that no information shall be retained unless it relates to criminal activity, how is that determination made on what is criminal activity?

Mr. DINH. Thank you for the question, Congressman. The determination is made by the agent initially and then approved by the supervisor, as in the normal course of any investigation.

Mr. KING. And then might it be retained if it potentially relates to potential criminal activity?

Mr. DINH. Yes, sir. What happens is that the agent would open a file, either a preliminary investigation or a full investigation based upon that indication of criminal or terrorist activity, and that file would remain open until the prosecution is brought or the investigation complete without charges.

Mr. KING. So, for example, if an agent went into a mosque and tape recorded a sermon in there and if some of the contents of that would have included some I'll say, inflammatory rhetoric, could that be something that could be compiled as potentially useful in a criminal investigation?

Mr. DINH. I think inflammatory rhetoric itself would not suffice, simply because one, not only is there an inadequacy of criminal activity, but more importantly there is a special sensitivity to the exercise of First Amendment rights. That agent conducting a public visit, first of all, would, under the guidelines, not be able to turn on the tape recorder. He would have to just simply observe on the

same terms and conditions as the public, and only when there is an indication of criminal activity would he be able to pursue other investigative avenues, including surreptitious recording.

Mr. KING. If they happened to be in a State that allowed for third-party tape recording, could they utilize that?

Mr. DINH. The utilization of surreptitious recording depends not on the laws of the State but the special procedures of the Department. Where it is a highly sensitive investigation, special sensitivity such as of a religious or political institution, there are special procedures in place in order to govern those sensitive activities, including ultimately review in certain cases by an undercover review committee.

Mr. KING. So in a case like Iowa, where if you and I are having a conversation, I can tape record that conversation? Would your guidelines prohibit that type of activity within Iowa?

Mr. DINH. The guidelines themselves would not prohibit it, but other—other administrative—and a memorandum governing the activity, the FBI may well have an

implication on it.

Mr. KING. So then at some point, if this—if we're going to compile a sense of intelligence about what might be going on domestically with regard to subversive activities, we may have to rely on third-party investigators, good citizens that utilize existing laws in a way that exceeds your ability to do so?

Mr. DINH. Certainly, informants have always been, and good citizens and good samaritans have always been a source of information investigative activity, as long as they do not act at the direction of FBI agents or under the authority of the United States Government. But independent of that, the Attorney General's guidelines liberate the ability of FBI agents to do what ordinary police, State and local police can do—that is, to identify threats on the same terms and conditions as members of the public generally.

Mr. KING. So if an interested person would then compile the text of, I'll say a series of meetings that advocated, without being, without being, without, I'll without leading toward violence but made those advocations, is that something that the Department could utilize?

Mr. DINH. As long as it was done not under the direction of or under the supervision or behest of the Government, there's nothing prohibiting us from getting such manna from heaven, as it were.

Mr. KING. And in fact, if there were a Web page that gathered that kind of information and posted it, it would be something that would be available to your Department?

Mr. DINH. Yes, and it would be as long as the Web page is publicly available, available to the FBI agents to search.

Mr. KING. Thank you, Mr. Dinh. Mr. Dempsey, you know, as I read your testimony, I'm just unclear as to your position, the portion where it says now FBI agents can apparently wander down the street and visit mosques or political meetings like anyone else, on a whim.

Am I to understand that you're opposed to that "on a whim" portion?

Mr. DEMPSEY. Yes. I believe that mosques and other political activities or religious activities are not off-limits, but that there has

to be some direction and guidance for FBI agents. Of all the mosques in the country, of all the political meetings, which ones do they go into? The Attorney General and, today, the Assistant Attorney General has repeatedly stated that FBI agents can do whatever members of the public can do, which is you walk down the street and say there's an interesting building, let me go in. Or you say—walk down the street and do it on a discriminatory basis, or do it on an arbitrary basis. I think that's a terrible allocation of resources.

I think also it does have a chilling effect. I think that an FBI agent is not an ordinary member of the public. He's not there as an ordinary member of the public. He's there specifically for a purpose. And unless that purpose is guided by the effort to collect information about potential terrorist activity, then I don't think he should be there.

Mr. CHABOT. The gentleman's time has expired.

Mr. KING. I appreciate your position on that. And thank you, Mr. Chairman.

Mr. CHABOT. Thank you. The gentleman from North Carolina is recognized for 5 minutes.

Mr. WATT. Thank you, Mr. Chairman.

Mr. Dinh, there have been posted in the Internet for some time something called PATRIOT II. Are you familiar with that?

Mr. DINH. I think on January 23 of this year the Center for Public Integrity did put up an unauthorized release of something and that was draft legislation purportedly from the Department of Justice. We do not——

Mr. WATT. Who did you say put it up?

Mr. DINH. The Center for Public Integrity.

Mr. WATT. And was that, was that a paper that originated in the Justice Department?

Mr. DINH. From all indications, yes, sir, it was a paper that was originated in and from the Justice Department. However, as we have made clear and as the Attorney General has made clear before the full Committee, that draft was exactly that: a draft that was still under the deliberative process, which was somewhat circumvented by the premature and unauthorized release of it.

Mr. WATT. And is the drafting process continually within the Department of Justice?

Mr. DINH. We are continuing trying to assess the way we do our business, because we know from specific evidence intercepted from communications of terrorist cells that they are watching us and evading our ability to prevent terrorist attacks. And so we're always thinking about new ways to do things effectively, and they include legislative proposals, executive amendments. I cannot say whether or if a specific legislative proposal will be made by the President, because ultimately it would have to be cleared through the Administration before any such proposals would be cleared. But we're constantly thinking about suggestions on how to improve our laws.

Mr. WATT. Have you eliminated from consideration any of the provisions that were posted on the Internet in that draft?

Mr. DINH. I'm sure we have, because as I said, it was a draft, it was a preliminary draft, that——

Mr. WATT. Which ones have you eliminated?

Mr. DINH. I cannot say with specificity, nor would I be at a position in order to identify those without going into more infringements of the deliberative process. I can say that it was a preliminary draft and so of course things will be added in and things will drop out. And indeed, decisions will——

Mr. WATT. Well, right now I'm trying to figure out which ones are being dropped out.

Mr. DINH. Frankly, if I was to answer your question, I would be engaging in the exercise of boxing against shadows, because I would not know which is in and which is out because the deliberative process is one that is continually evolving. And until we have a final draft that is approved by the Administration and the Attorney General, I would not be at liberty to discuss any specific provisions.

Mr. WATT. You're part of that ongoing process?

Mr. DINH. Yes, I am part of that ongoing process, as well as a number of people within the Department of Justice and elsewhere.

Mr. WATT. Let me ask this question, Mr. Dinh. What things have you found from your own experience that you believe are not currently authorized in PATRIOT, the PATRIOT Act, that you believe should be being considered whether they get proposed or not?

Mr. DINH. I guess the safest way for me to answer that question is to refer back to the January 19 Center for Public Integrity draft. And that draft, as it is public, includes a provision which amends the FISA statute to take care of the Moussaoui problem, the so-called "lone wolf" fix. Senator Kyl and Senator Schumer in the United States Senate have proposed a similar measure, and that is a measure that the Administration has endorsed. And that's another example.

Mr. WATT. How would that work?

Mr. DINH. Right now, in order to be subject to the FISA regime as opposed to the criminal surveillance, you would have to be an agent of a foreign power. And a foreign power is defined to include foreign nations, obviously, but also international terrorist groups. At a beginning of an investigation, as was the case with Moussaoui, we do not know whether Mr. Moussaoui was acting on behalf of a—in connection with a terrorist group or alone. We now obviously know, or at least we are—we present evidence and allege that he was part of an international conspiracy. At the beginning of an investigation, that bill would allow FISA be used even if there were no specific connection to an international terrorist group.

Mr. WATT. So in effect that would allow the U.S. Government to go after any individual anywhere in the world, whether they were acting independently or on behalf of another nation?

Mr. DINH. Not any individual, not anywhere around the world. It does allow the Government to go after lone-wolf terrorists and spies, because the damage done by a single person can be as devastating as——

Mr. WATT. I don't mean to be semantic, but is there some difference between a lone wolf and any individual who might be engaging in some kind of——

Mr. CHABOT. The gentleman's time has expired, but the gentleman can answer the question.

Mr. DINH. Yes, sir, thank you very much, Mr. Chairman, for the accommodation. First of all, the amendment in the Kyl-Schumer bill only applies to non-U.S. persons, and so it's——

Mr. WATT. To?

Mr. DINH. Non-U.S. persons. And so it would take out a majority of the population within the United States. Also, that person would have to be engaging in terrorist activity, international terrorist activity as defined by statute or intelligence.

Mr. WATT. So whoever you all say is a lone wolf is a lone wolf——

Mr. DINH. No, sir, not in——

Mr. WATT.—as opposed to just anybody?

Mr. DINH. No, there is judicial supervision of application of the standards. In order to engage international terrorist activity, you have to knowingly engage in certain activities that is in violation of the laws of the United States and also with the intent to coerce and intimidate governmental policy. In order to engage in clandestine intelligence activities, you have to knowingly engage in activities that violate the laws of the United States and also to—relating to intelligence collection. So it's not just anybody doing anything. It's very particularized, subject to approval by judges who are article III judges.

Mr. CHABOT. The gentleman's time has expired. The gentleman from Florida, Mr. Feeney, is recognized for 5 minutes.

Mr. FEENEY. Thank you, Mr. Chairman. Mr. Dinh, in the first place, the two individuals that you were just being—the cases that you were being asked about a little bit earlier with the—with respect to the Department of Defense designation, were those U.S. citizens that were so designated?

Mr. DINH. Both, sir. Mr. Hamdi was a U.S. citizen who was captured on the battlefield in Afghanistan. Mr. Jose Padilla is a U.S. citizen who was captured in the Chicago O'Hare Airport, and our evidence indicates—and this was made in an affidavit submitted in court—indicates that he came to the airport with the intention of detonating a dirty bomb in the vicinity.

Mr. FEENEY. I appreciate that. I'm also interested in whether or not there's anything in the PATRIOT Act or any other aspect of Federal law that would permit any of the Executive Branch offices to designate an individual U.S. citizen in such a way that that individual would lose any of their otherwise protected freedoms under the Constitution or the Bill of Rights.

Mr. DINH. No, sir, nothing in the laws or specifically in the United States—or in the USA PATRIOT Act. As our pleadings make clear, the President was acting under his authority, his executive authority as commander in chief.

Mr. FEENEY. And there are exceptions under article I, section 9 in terms of suspending habeas corpus, is that right? I think invasion of the public safety and domestic rebellion, or——

Mr. DINH. Yes, sir, you are absolutely correct. And those are the provisions that President Lincoln relied upon in order to suspend habeas corpus and declare martial law during the Civil War. And this is in answer to Mr. Scott's earlier question, that the President

obviously has not made such a determination nor does he have intent, present intent to do so.

Mr. FEENEY. Well, even if we are under a current rebellion or invasion of the public safety, other than habeas corpus, I'm not aware of any other rights that any U.S. citizen may be forced to forfeit as a consequence of such a designation.

Mr. DINH. Nor am I, sir, just the great writ of habeas corpus is the specific suspension clause.

Mr. FEENEY. Well, and Professor Kerr, I guess other big portion of the Constitution we've talked about today would be the Fourth Amendment. And of course the proscription against searches or seizures is against—is limited; it's against unreasonable searches and seizures. And so maybe you could describe briefly for me the way the Court has evolved during certain periods of national crisis with protecting the right of individuals not to be unreasonably subject to searches or seizures, and how that has been affected and how those Court precedents may affect the situation we're in today, where the terror threats are at an all-time high.

Mr. KERR. Of course. There's been an evolution in the Supreme Court's jurisprudence in the Fourth Amendment over time. The general explanation which the cases support is that originally the Fourth Amendment was very concerned with protecting property rights, and in sort of moving through the 1960's and, really, in the *Katz* v. *United States* case, moving toward more of a privacy-protecting approach.

At the same time, the Supreme Court has been more deferential in the context of wartime, for example, or especially in the area of national security, than in criminal investigations. So for example, in the Keith case in 1978, I believe, the Supreme Court recognized that the Fourth Amendment did apply in domestic national security related cases, but suggested that Congress could carve out a new set of rules which might be different from the traditional Fourth Amendment standards that would apply in criminal cases.

So the Court has been, I think, fairly pragmatic in this area and suggested that it's really up to a question of what is the threat, what are the reasonable steps that can be taken in response to it? But at the same time, it is a fairly unclear area of law. The Court has not had that many opportunities to step in and clarify the rules.

Mr. FEENEY. Well, thank you. And finally, Mr. Rosenzweig, I think a lot of the panel members and the Members have voiced support for the notion that we've got some 4-year sunset provisions on a lot of the applications. Maybe because I'm familiar with the Heritage's philosophy and tend to endorse it on most issues, maybe my experience at the State level may be relevant, because I used to believe I was for sunsetting every part of the chapter and code in the statute book. But what I found was that every interested party and group in the world, when they were aware that that sunset was coming up, and we were able on a routine basis to turn about three pages of the statutes into 203 pages by the time we were done sunsetting provisions. So we may get what we asked for on this one.

Mr. ROSENZWEIG. I would not support sunsetting every provision of every law, for precisely the same reasons that you've just alluded

to, that it gives us the opportunity for a big Christmas tree to be grown in the midst of Congress. In the context, however, of this vital issue, the balance between civil liberty and national security, one that I think is, frankly, the most important legal issue, domestic legal issue facing this Congress this year—more important than Medicare, more important than Social Security. The importance of getting it right and the importance of keeping Congress engaged is, in my judgment, sufficiently great that artificial mechanisms like the sunset are, I think, to be used cautiously, judiciously. Also, to be candid, I think on this type of provision, there's pretty unlikely there are going to be a lot of Christmas trees. As Patriot—as the next PATRIOT Act goes through, nobody's going to put a tax break on—I hope.

Mr. FEENEY. Well, but you just heard PATRIOT II described by one of my colleagues——

Mr. CHABOT. The gentleman's time has expired. The gentlelady from Texas, Ms. Jackson Lee, who is a Member of the full Committee but not a Member of this Committee, has asked for 2 or 3 minutes to ask questions. She's assured me she'll stay within that time. If there's no objection, I will grant the lady two and a half minutes, and as long as she'll stay within that time, we will grant her that. Are there any objections?

[No response.]

Mr. CHABOT. If not, the gentlelady is granted that time.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman. And I know that your monitoring the clock will help me.

I thank the witnesses very much. And with this time, I need simply to make some comments and requests as well. I'm gratified that the statement of the Chairman recites the Fourth Amendment provides that the right of the people to be in secure in their persons, houses, papers, and effects against unreasonable searches and seizures and that it should not be violated. Let me get on the record my opposition to any PATRIOT II without a full hearing and briefing and an assessment and an accounting on the impact of PATRIOT I, particularly if there are far reaches and expansion and—under—and an undermining of the Fourth Amendment.

Might I remind my friends and colleagues of Ruby Ridge and Waco. These are incidences that occurred before 9/11, and I think it's important to know that this is a far-reaching issue. Beyond immigrants and beyond Arab—the Arab community and Muslim community, this is an American question of whether or not our constitutional rights have been infringed upon.

Secondly, let me raise a question that's pertinent to Texas, and thank the Justice Department for responding quickly to my question as to whether or not there was any criminal violation by the 55 legislators who went to Ardmore and other places in Texas. A letter came back, and I'm very grateful for that, indicating there was no Federal question or Federal need for intervention. The DOJ did not see that need.

In light of that, I would appreciate it greatly, as we are asking the Homeland Security provide us with all tapes, and we have seen that the Inspector General has recused himself and another person investigating, I'm making an official request that the DOD do a separate investigation with respect to the question of whether the

Republican Party, the majority leader, or any person employed by them or acting on their behalf contact the Department of Justice or the Department of Homeland Security or any agency acting under their auspices seeking the assistance of a Federal agency resources to locate any Democratic member of the Texas State legislature.

Again, I believe this ties into our inquiries today. And I would appreciate whether or not you would give a response to the fact that any action by the Texas legislature was a detriment to the public and whether or not the public's civil liberties were in question if that occurred.

Lastly, Mr. Chairman, so that I can keep within the time frame——

Mr. CHABOT. The gentlelady's time has expired and the gentlelady's request has been duly noted.

Ms. JACKSON LEE. Thank you. And I'll provide the others in writing. I thank you very much, Mr. Chairman, for the time.

Mr. CHABOT. Thank you. The gentleman from New York has also asked unanimous consent to ask one additional question, and if there's no objection, the gentleman is granted that.

Mr. NADLER. Thank you, Mr. Chairman.

Let me say the following first, then ask my question. In discussion with Mr. Scott some of his questions—I'm sorry, with Mr. Watt, his questions—or no, it was Mr. Scott. I'm getting confused here. You were discussing the Administration's position in the Hamdi and Padilla cases. And the fact is—the fact is that the Administration took the position, and if you look at your brief you'll see it, that when the President or the Department of Defense has designated an American citizen or anyone else an enemy combattant, the courts have no jurisdiction, no jurisdiction, to question that designation. The courts have not agreed with that, but that's the Administration's position. And that's a claim of power, a claim that habeas corpus doesn't exist, that nothing exists, that the President in that decision is all-powerful, that nobody, until that brief, had made in an English-speaking jurisdiction—before Magna Carta. And I would point out that this country rebelled against Great Britain for tyrannical assertions far less grievous than that.

My question, however, is on a different—and that's the record, if you look at the brief of the Justice Department. There's no question. In saying that habeas corpus exists, it only exists because the court didn't agree with the Administration.

My question is the following. Getting back to FISA, the whole point of FISA is that the Fourth Amendment says you can't search—you can't issue a search warrant, basically, unless there's probable cause to believe that a crime was committed, or maybe it had to be committed. FISA, however, says wait a minute, when you're dealing with foreign intelligence agents and you're not talking about a criminal prosecution but fighting an intelligence war with the Soviet Union or al Qaeda whoever, you shouldn't adhere to that standard. The PATRIOT Act comes along and says—and that's for a foreign intelligence investigation. The PATRIOT Act comes along and says that, well, you can adhere to a lesser standard than the Fourth Amendment requires if foreign intelligence is a significant purpose—not the only purpose or the main purpose,

but a significant purpose. The Department, in its answers to various questions of this Committee, has said that they've used various of these powers on drug cases and other cases.

My question is, if you are allowing use of FISA standards, which is less than Fourth Amendment standards, for questions which aren't really foreign amendment—foreign intelligence, but for crimes, what is left of the Fourth Amendment?

Mr. DINH. You ask a very good question. I would like to discuss that in detail——

Mr. NADLER. And—excuse me, let me just say—and how can we do that constitutionally and say the crimes can be—criminal investigations, even if there's some foreign intelligence thing, can be governed by a less-than-Fourth-Amendment standard? Whatever you decide the Fourth Amendment means, how can you say it's governed by less than the Fourth Amendment?

Mr. DINH. I completely understand. With respect, Mr. Congressman, I am advised that in the Hamdi case, we did not move to dismiss the habeas petition, but simply argued that the designation was conclusive, consistent with Ex Parte Qurin. In Padilla, we did make a——

Mr. NADLER. And—excuse me—and if—go ahead.

Mr. DINH. In Padilla, we did make a motion to dismiss for lack of personal jurisdiction because we thought that Mr. Padilla, who was being held in South Carolina, venue was in South Carolina.

Mr. NADLER. Well, forget the venue. But even your first thing, if you say the court lacks jurisdiction, then there can be no habeas.

Mr. DINH. No, sir, we did not move to dismiss on lack of jurisdiction. We argued that under the law, Ex Parte Quirin in particular, the designation as enemy combattant is conclusive upon the——

Mr. NADLER. Excuse me, the designation is conclusive; therefore there is no habeas corpus or anything else. The designation——

Mr. DINH. No, here's——

Mr. NADLER. Wait a minute. The designation is con—if you say the designation is conclusive, and once that designation is conclusive, then there is no right to habeas corpus, correct?

Mr. DINH. We are in agreement in all but characterization. Habeas petition exists, he can present all his arguments legal and factual. It just so happens that under the law, his habeas argument is not worth very much. The habeas petition would be dismissed not for want of jurisdiction, but for want of substance.

Mr. NADLER. I find that, frankly—what's the word I'm looking for?—sophistry.

Mr. DEMPSEY. All he's saying is, is that the President declares that you're an enemy combattant, the facts of the law do not matter after that, that the only law that matters is their reading of the law that the President can do this.

Mr. DINH. No, the law as interpreted by the Supreme Court is the law that the court applied in this case and in all other habeas cases, and it just so happens that the——

Mr. NADLER. Is that what they said in Quirin? That's not—but in other words, what you're saying is once the President decides that you're an enemy combattant, you can make a motion to habeas corpus but it doesn't matter what the facts are and it doesn't matter what the law is. The designation is conclusive and——

Mr. DINH. It absolutely matters what the law is. And the law is that——

Mr. NADLER. That you have not right——

Mr. DINH.—the President is due substantial deference, because courts are an imperfect place to make these kinds of judgments that the Executive made.

With respect to your FISA question, it is an extremely important question, a very good constitutional question. As you know, FISA was adopted by Congress in response to the Keith decision that Professor Kerr has elucidated before. It governs very, very strictly the conduct of counter-intelligence and intelligence and it has very specific procedures that govern the use of such information in a subsequent criminal proceeding. For example, before FISA-derived information can be used "before any court, department, officer, agency, regulatory body or other authority of the United States," notice has to be given to the interested party, that is, the person who is the defendant. That party then has the ability to file a motion to suppress or to discover such information underlying the FISA application. Under those proceedings are when the arguments of Fourth Amendment would be aired in the subsequent use.

The reason why this system exists and is fully constitutional is that the Court, in *Keith* and in other cases, has held that the warrant requirement, that is, the warrant of probable-cause, the requirement of the Fourth Amendment, does not apply to these orders, but rather reasonableness applies. And as the court of FISA review made clear, that standard of reasonableness differs from the probable cause requirement of the warrant clause of the Fourth Amendment.

Mr. CHABOT. The gentleman's time has expired.

Mr. NADLER. I thank the Chairman for his courtesy and indulgence.

Mr. CHABOT. The Chairman duly notes that. A request has been made—the gentleman over here, Mr. King, would like to ask some questions in light of the gentleman—I don't want to open this up for a whole second round, but Mr. Schiff has come in, and as a compromise, I would let Mr. Schiff also ask questions after Mr. King. But I really don't want to go into an entire second round.

The gentleman from Iowa is recognized for his question.

Mr. KING. Thank you, Mr. Chairman. And I wouldn't raise this issue if it hadn't been raised in this hearing. But it has been raised. And I direct my question to Mr. Dinh. And that is that with regard to the gentlelady from Texas' remarks and questions regarding the Federal involvement in the legislature in Texas. And I would just expand on that. I understand the position you've taken today. But should the minority in the Texas legislature just simply stay out of the State of Texas, where then they would succeed in thwarting the will of the people of the State of Texas, and if that went on indefinitely, it would simply just shut down the entire legislature of Texas indefinitely. So would you or would your Department foreclose any Federal involvement should that ultimately be the case?

Mr. DINH. We don't foreclose any such thing. Of course, I'm not familiar with the facts nor of any eventuality, so I cannot speculate on that. But we never say never to anything.

Mr. KING. Thank you, Mr. Dinh. Thank you, Mr. Chairman.

Mr. CHABOT. The gentleman yields back. The gentleman from California, Mr. Schiff, is recognized.

Mr. SCHIFF. I thank the Chairman for the opportunity. I want to make a couple of quick points and then I have a couple of questions to ask. And I ask these as someone who sponsored the PATRIOT bill and felt that many of the changes were necessary to keep pace with changes in technology and the use of that technology by terrorists. Nonetheless, some of those changes, although necessary, require much more vigilant oversight by the Congress. And as a former assistant U.S. attorney very familiar with the Justice Department, I would have felt that way as a member of the Justice Department. I certainly feel that way as a Member of Congress. So we have to do a much more vigilant job, I think, as Members of this Committee than we have in the past. And I know that some of the questions, many of the questions that have been posed by the Committee on a bipartisan basis have not received very full or forthcoming answers. And that's of great concern. And I understand that some of the information is classified. And I understand earlier today there was a representation made that some of the responses will be provided to the Intelligence Committee. I'd like to propose that we have a classified hearing of this Committee. Because in addition to the Intelligence Committee's interest, this Committee has, I think, primary interest over the potential deprivation of people's civil liberties and civil rights. And I think that we ought to have an unencumbered and classified forum where we can ask questions about how often have library records been searched, under what circumstances, with what result, and get straight answers and not have to navigate through other Committees or other processes to do that.

The second point I'd like to make is in the area of detention, because I think both in the original PATRIOT proposal and in the amended PATRIOT proposal that subsequently passed the Congress, and in the conduct of the Administration outside of the confines of the PATRIOT bill—and much of what concerns me has been outside the confines of the PATRIOT bill—there are some very, I think, alarming decisions that have been made in the area of unlawful enemy combatants, and that is the Administration taking the position that it can unilaterally designate someone, an American, as an unlawful enemy combattant and deprive them of access to counsel and access to the courts. I think that is really unprecedented accretion of authority by the Executive. If I were still in the Justice Department and I were asked, "Do you want the authority to unilaterally pick someone up off the street, call them an enemy combattant, and have your decision unreviewable?" I would say no. And I don't think any one branch of Government ought to have that power.

I've introduced a bill to provide some very basic requirements, like access to counsel and access to court, and allow the Department to promulgate regulations about how that could be accomplished and maintain the interests of the country and national security. But we have to find a method to provide some form of meaningful judicial review of the detention decisions. I think it's in

the Department of Justice interests, I think it's in the country's interest. So I ask you to give that your consideration.

Finally, on the PATRIOT II potential bill on the proposal that was aired in the Senate—it may have been withdrawn in the Senate—to advance the sunset date of the PATRIOT bill, I think that the Justice Department is going to have a lot of work to do in being much more forthcoming in information about how the first PATRIOT bill has been implemented before it ought to request anything further from the Congress and certainly anything further from anyone who supported the first PATRIOT bill. And I would not recommend at this point, in either house, seeking to advance the sunset date, because there are still a great many unanswered questions. And I would just ask for your response.

Mr. DINH. Thank you very much, Congressman. You are a good friend of the Department and an illustrious alumnus of the U.S. Attorney's Office in Los Angeles. I recently talked to Deborah Yang, and she sends her regards. And all your colleagues miss you there tremendously.

We do take congressional oversight very, very seriously. We believe in it, especially in a highly charged investigation such as this. We think that it's incumbent upon us to present you with as much information as possible. That is why we recently—last week—provided 60 pages of answers to the bipartisan questions that were submitted to the Department.

With respect to the section 215 business-records provision in particular, that requires a semi-annual report to both this Committee and the Intelligence Committee. I am advised that we did make that report on a timely manner for the last 2 years. The last one was in October of this last year. And I'm advised further that we are finalizing the next report. That will be provided to this Committee in a classified setting per your request, and I should be happy to provide that classified information, or my colleagues will, to you personally also.

As I have said in answer to Congressman Watt, we are constantly evaluating the way we do our job, to make sure that we have all the authorities we need in order to protect America and the safety of her people. Until there is, whether there is a final proposal, I would not be in a position to comment on it except to say that I agree with you that we will fully cooperate on your task of overseeing how we have implemented, utilized to great success the authorities you have given us in the USA PATRIOT Act.

Mr. CHABOT. The gentleman's time has expired. The gentleman from Virginia has requested one final question, and without objection he will be granted that opportunity.

Mr. SCOTT. Thank you, Mr. Chairman. I just wanted to make a quick statement before I asked a question, and that is to quote language out of—quote some language for Mr. Dinh. "It is well settled that the military has the authority to capture and detain individuals who it has determined are enemy combatants. Such combatants, moreover, have no right of access to counsel to challenge their detention. The courts have an extremely narrow role in challenging the military judgment to detain an individual as an enemy combattant. A court's inquiry should come to an end once the military has shown that it has determined that the detainee is an

enemy combattant. The court may not second guess the military's enemy combattant determination. At the very most, given the separation of constitutional powers in this unique area, a court should only require the military to point to some evidence supporting its determination. Either way, no evidentiary hearing is required to dispose of a habeas petition in this military context."

Before you comment on that, let me just ask a question. If you have gathered through this data mining process some information—Mr. Dempsey suggested that it gets passed all around to whoever wants it. I noticed on page 47 of the answers that a group called ChoicePoint has been designated as one of the groups you get information from. I guess my question is, does that have anything to do with the Florida voting situation? Is that the same group? And who gets to look at the information that's gathered? If you're an innocent person at a library, does my next-door neighbor who happens to work for the FBI get to look at everything I have gotten from the library just because a terrorist may have used the same library?

Mr. DINH. Thank you very much, Congressman. I fully agree with what you've read, and there again, we agree. On what the Government argued, I would like to read the portion that immediately precedes that. It says very clearly that "the writ of habeas corpus remains available to individuals, such as Hamdi, who are detained as enemy combatants to challenge the legality of their detention." As I have answered Mr. Nadler's question, our position is that the writ of habeas corpus remains open. But as you have read in our portion of the brief, we believe that the law governing such habeas corpus in the case of enemy combatants is highly limited and the Judiciary gives substantial deference to the Executive.

With respect to your question regarding the use of——

Mr. SCOTT. That wasn't deference. That has—is not review, "may not second guess."

Mr. DINH. Yes, sir, only as long as we come up with some evidence. That is the existing law as we believe it to be. The 4th Circuit has agreed with us, and we are in litigation in the 2nd Circuit—not on this precise point, because I think the law is clear from the Supreme Court.

With respect to the use of information systems, I do not know to which Florida issue you refer, but ChoicePoint is a commercially available database. That data is not data flowing from the Government to the private sector. That is data collected by the private sector for use by the private sector, and available for use to the Government in its law-enforcement purposes. When the Government collects data for law enforcement purposes or other purposes, its use of that data is governed by the applicable law. And most of that prohibits the disclosure of such information to the private sector. So, for example, our investigative files are not available. We do not make that data available to the general public.

Mr. SCOTT. I'm talking about people that work for the FBI. If my next-door neighbor works for the FBI, do they get to read what books I took out of the library because they have data mined the library and gotten all the information? You're not releasing it publicly, just all the employees get to review what I took out. Is that right?

Mr. DINH. No, sir. The investigative files are tightly controlled, but precisely for the privacy—the issues that you have highlighted. Even as we authorize the use of information systems and other technology in the Department of Justice and the FBI with the Attorney General guidelines, we have made clear that existing regulations concerning the use of such information systems adhere. And so it has to be authorized for specific purposes. And a big challenge is our development of systems in order to select those who are authorized versus those who are not. And all of such access is recorded for subsequent disciplinary or repository use.

Mr. SCOTT. Thank you. If Mr. Dempsey could just make a brief comment on that?

Mr. DEMPSEY. There have been problems with FBI agents and other IRS officials, and others obtaining unauthorized access, and that is something that needs to be subject to careful controls, audit trails, internal investigations. Just recently I think two FBI agents were accused of, I think, basically running a little business on the side of selling information from FBI files, that DEA, all the agencies have been subject to that.

The other half of the question is the authorized use and disclosure question. The way the laws now work there are very little limits on authorized disclosure where it's in the name of counterterrorism or law enforcement. The Defense Department right now is building a major new information sharing system intended to make that easier. The Department of Homeland Security has a role, the other entities being set up. Those need to have the rules put in place on how this private sector data comes into Government hands, data that has accuracy problems, that may have relevancy problems, data that may be incomplete. When you draw that in or when the Government pings that database or when the Government subscribes to that database, there are huge unanswered questions about accuracy, control, reuse, retention, dissemination, interpretation. Those rules need to be developed. They are not there now.

Mr. CHABOT. The gentleman's time has expired.

Mr. SCOTT. I appreciate it, Mr. Chairman. Thank you.

Mr. CHABOT. Thank you.

There is a vote on the floor. When the PATRIOT Act was passed, assurance was given that there would be congressional oversight and that we would look into how this law was being implemented. This hearing today has been part of this process. We appreciate the panel's contribution to that effort.

I would ask unanimous consent that all Members may have five legislative days in which to revise and extend their remarks and to include extraneous material.

If there is no further business to come before this Committee, we're adjourned.

[Whereupon, at 3:50 p.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

June 2, 2003

Mr. Viet D. Dinh
Assistant Attorney General
Office of Legal Policy
Department of Justice
950 Pennsylvania Avenue N.W.
Washington, DC 20530

Dear Assistant Attorney General Dinh:

On behalf of the Committee on the Judiciary, Subcommittee on the Constitution, I want to express our sincere appreciation for your participation in the May 20, 2003 oversight hearing on the Patriot Act. Your testimony will greatly assist us in future deliberations on the many important issues addressed during the hearing.

Please review the **verbatim** transcript which Michael Bell had someone pick up on May 29, and submit any edits that you may have to the Subcommittee on the Constitution by *June 11,2003.* Due to the current mail situation, please fax those pages with edits to the attention of Catherine Graham at (202) 225-3746.

The Committee's Rule III (c) pertaining to the printing of transcripts is as follows:

> *The transcripts . . . shall be published in* ***verbatim form****, with the material requested for the record . . . as appropriate. Any requests to correct any errors, other than transcription, shall be appended to the record, and the appropriate place where the change is requested will be footnoted.*

I also have enclosed additional questions for you. Please return your response in writing via fax or email (catherine.graham@mail.house.gov) by July 2 for inclusion in the published transcript of the hearing.

If you have any further questions or concerns, please contact Catherine at (202) 226-7680. Thank you again for your testimony.

Sincerely,

STEVE CHABOT
Chairman

Enclosure

SC/cg

Written question for submission by Chairman Chabot to Assistant Attorney General Dinh
May 20, 2003 Oversight Hearing, House Judiciary Constitution Subcommittee

- The USA PATRIOT Act, 18 U.S.C. § 3123(a)(3), requires the government to maintain reports of "the configuration of and duration of each time" a program such as Carnivore is installed and "any information which has been collected by the device." Under what circumstances would a Member of Congress or a Congressional committee be able to review these reports?

- The 2002 revisions to the FBI Guidelines provide that "For the purpose of detecting or preventing terrorist activities, the FBI is authorized to visit any place and attend any event that is open to the public, on the same terms and conditions as members of the public generally. No information obtained from such visits shall be retained unless it relates to potential criminal or terrorist activity." I understand from your testimony that each FBI field office retains a "control file" that contains information on how agents use their time, including the time they spend at events open to the public, on the same terms and conditions as members of the public generally. Under what circumstances, and by what procedure, would a Member of Congress or a Congressional committee be able to review the number of FBI agent visits to and the amounts of time FBI agents spend at such events open to the public?

- Under the USA PATRIOT Act's amendments to the Pen Register Statutes, is it your understanding that all non-"content" information is "dialing, routing, addressing, and signaling" information under 18 U.S.C. § 3127(3), so that all such "dialing, routing, addressing, and signaling" information can be gathered only under the authority of the Pen Register Statute? Or is there a third category of information outside of "contents" (defined in 18 U.S.C. § 2510(8)) and "dialing, routing, addressing, and signaling" information, such that its collection by the government falls under neither the authority of the Pen Register Statutes nor the Wiretap Act (which require the government to obtain a warrant to gather the "contents" of communications)? If there is such a third category of information, what statutory provisions or Department rules and procedures govern its collection by the Department of Justice?

- It's my understanding that the first FBI Guidelines and all subsequent Guidelines changes were adopted only after consultation with the House Judiciary Committee. What was the reason for breaking that tradition when the 2002 FBI Guidelines were adopted?

U. S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

July 31, 2003

The Honorable Steve Chabot
Chairman
Subcommittee on the Constitution
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

We have enclosed responses to written questions posed to the Department following the appearance before the Subcommittee of then-Assistant Attorney General Viet Dinh on May 20, 2003. The subject of the hearing was oversight of the USA PATRIOT Act.

We hope these responses are helpful to you. Please do not hesitate to call upon us if we may be of additional assistance.

Sincerely,

William E. Moschella
Assistant Attorney General

Enclosure

cc: The Honorable Jerrold Nadler
Ranking Minority Member

Responses to Questions by Congressman Steve Chabot
to Assistant Attorney General Viet D. Dinh

Question: The USA PATRIOT Act, 18 U.S.C. § 3123(a)(3), requires the government to maintain reports of "the configuration of and duration of each time" a program such as Carnivore is installed and "any information which has been collected by the device." Under what circumstances would a Member of Congress or a Congressional committee be able to review these reports?

Response: Congress has required that reports about the use of these devices be treated with confidentiality because they contain sensitive information about pending criminal investigations, and their disclosure could endanger the integrity of ongoing cases, as well as the privacy of investigation subjects. Specifically, pursuant to 18 U.S.C. § 3123(a)(3)(B), the records maintained under 18 U.S.C. § 3123(a)(3)(A) must be provided under seal to the court which entered the order authorizing the installation and use of the device. In some instances, courts enter orders that further restrict dissemination of the information contained in the reports. These reports could not be provided outside of the normal judicial proceedings unless the court authorized such release.

Question: The 2002 revisions to the FBI Guidelines provide that "For the purpose of detecting or preventing terrorist activities, the FBI is authorized to visit any place and attend any event that is open to the public, on the same terms and conditions as members of the public generally. No information obtained from such visits shall be retained unless it relates to potential criminal or terrorist activity." I understand from your testimony that each FBI field office retains a "control file" that contains information on how agents use their time, including the time they spend at events open to the public, on the same terms and conditions as members of the public generally. Under what circumstances, and by what procedure would a Member of Congress or a Congressional committee be able to review the number of FBI agent visits to and the amounts of time FBI agents spend at such events open to the public?

Response: Part VI(A)(2) of the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations ("Part VI(A)(2)") authorizes FBI agents to visit public places and events for a single purpose – "detecting or preventing terrorist activities" – and require that such visits take place "on the same terms and conditions as members of the public generally." The guidelines sharply restrict agents' ability to collect or maintain information resulting from these visits. In particular, the FBI is flatly prohibited from retaining any information that does not relate to criminal wrongdoing: "No information obtained from such visits shall be retained unless it relates to potential criminal or terrorist activity." Consistent with this directive, the FBI does not maintain detailed information about visits to public places that have not produced information relating to criminal or terrorist activity.

While the FBI does not require centralized reporting of agent visits to public places and events, some administrative information about these visits may be maintained on an

informal basis. When an agent conducts such a visit pursuant to Part VI(A)(2), and does not obtain information related to terrorism or criminal activity, he or she should document the date, time, and place of the visit, as well as the fact that the visit did not produce any relevant information. This documentation is not filed in an investigative file (because it does not relate to a specific investigation), but it can be retained in a "control file." Control files are administrative tools used at the discretion of managers in FBI field offices for organizational purposes, to act as repositories of information related to the investigative program for which the managers have oversight responsibility.

Control files may reflect that public places have been visited pursuant to the Part VI(A)(2) authority, and when those visits took place, but there is no single set of documents indicating the number of visits to public places or the amount of time agents spend at such public places. In part, this is because control files are maintained on a decentralized basis in individual FBI field offices. Moreover, managers in field offices have discretion as to the type and content of their control files. Thus one supervisor may keep documentation relating to a Part VI(A)(2) visit in a control file along with other sensitive counterterrorism information, while a supervisor in another field office might maintain a control file solely devoted to agent visits to public places.

Although there is no centralized repository of documents containing information about FBI visits to public places and events, in the past, information about these visits has been obtained through an informal survey of field offices. For example, the Department of Justice received a letter, dated April 1, 2003, from the Chairman and Ranking Member of the House Judiciary Committee that posed questions about USA PATRIOT Act implementation and related matters. On May 13, 2003, Acting Assistant Attorney General Jamie Brown submitted the Department's responses, which included information about visits to certain public places that FBI Headquarters gathered informally from field offices.

Question: Under the USA PATRIOT Act's amendments to the Pen Register Statutes, is it your understanding that all non-"content" information is "dialing, routing, addressing, and signaling" information under 18 U.S.C. § 3127(3), so that all such "dialing, routing, addressing, and signaling" information can be gathered only under the authority of the Pen Register Statute? Or is there a third category of information outside of "contents" (defined in 18 U.S.C. § 2510(8)) and "dialing, routing, addressing and signaling" information, such that its collection by the government falls under neither the authority of the Pen Register Statutes nor the Wiretap Act (which require the government to obtain a warrant to gather the "contents" of communications)? If there is such a third category of information, what statutory provisions or Department rules and procedures govern its collection by the Department of Justice?

Response: The Department of Justice interprets the phrase "dialing, routing, addressing, and signaling information," which is used throughout the pen register and trap and trace statute (18 U.S.C. §§ 3121 et seq.), as complementary to the term "contents," as defined in section 2510(8) of the Wiretap Act. Thus, where law enforcement seeks court authorization

to obtain the "contents" of a communication, it may not do so under the auspices of the pen/trap statute, but rather under the authority of the Wiretap Act. Further, we do not believe that there exists a third category of information which is not comprehended by either "contents" or "dialing, routing, addressing, and signaling information."

Question: It's my understanding that the first FBI Guidelines and all subsequent Guidelines changes were adopted only after consultation with the House Judiciary Committee. What was the reason for breaking with that tradition when the 2002 FBI Guidelines were adopted?

Response: The Department of Justice is fully committed to consulting with Congress on how to most effectively wage the war on terrorism while preserving Americans' civil liberties. In the aftermath of the September 11 terrorist attacks, Justice Department officials regularly met with Members of Congress and their staffs in an effort to equip law enforcement with the tools they need to prevent future acts of terrorism. The USA PATRIOT Act was one product of those consultations.

The Attorney General's investigative guidelines reflect the Attorney General's administrative responsibility as head of the Justice Department to provide guidance to the Federal Bureau of Investigation. The rules and restrictions the guidelines impose supplement the legal requirements enacted by Congress.

We cannot confirm that all previous changes to the Attorney General's guidelines were adopted only after consultation with the House Judiciary Committee. The guidelines have undergone many revisions since they were first issued in the 1970s. The original guidelines, issued by Attorney General Edward H. Levi, were preceded by congressional hearings into alleged abuses by the FBI, as well as by consultation between the Executive and Legislative branches in an effort to ensure that such abuses did not recur. We cannot confirm that any consultations took place when the guidelines subsequently were revised.

Justice Department employees promptly briefed congressional staff when the revised guidelines were issued in 2002. Since then, extensive additional information about the guidelines' purpose and operation continues to be made available through legislative hearings, follow-up questions from those hearings, and other inquiries from Congress.

LEGAL BRIEF SUBMITTED BY REP. ROBERT C. SCOTT

No. 02-6895

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

YASER ESAM HAMDI, et al.,

Petitioners-Appellees

v.

DONALD RUMSFELD, et al.,

Respondents-Appellants.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

BRIEF FOR RESPONDENTS-APPELLANTS

PAUL J. McNULTY
United States Attorney

PAUL D. CLEMENT
Deputy Solicitor General

ALICE S. FISHER
Deputy Assistant Attorney General

GREGORY G. GARRE
Assistant to the Solicitor General

LAWRENCE R. LEONARD
(757) 441-6331
Managing Assistant United States Attorney

United States Department of Justice
950 Pennsylvania Avenue, N.W.

Washington, D.C. 20530-0001

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 02-6895

YASER ESAM HAMDI, et al.,

Petitioners-Appellees

v.

DONALD RUMSFELD, et al.,

Respondents-Appellants.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

BRIEF FOR RESPONDENTS-APPELLANTS

JURISDICTIONAL STATEMENT

Petitioners invoked the jurisdiction of the district court under 28 U.S.C. 2241. The district court entered an order on June 11, 2002 (reproduced in the addendum hereto), requiring, inter alia, respondents to provide the federal public defender with private, unmonitored access to the detainee. Respondents filed a timely notice of appeal of that order on June 13, 2002, and an emergency motion for a stay pending

appeal. The Court granted respondents' stay request on June 14, 2002. This Court has jurisdiction under 28 U.S.C. 1292. In addition, the Court would have jurisdiction under 28 U.S.C. 1651. See Jamison v. Wiley, 14 F.3d 222, 234 (4th Cir. 1994) (court may treat notice of appeal as petition for a writ of mandamus).

STATEMENT OF THE ISSUE PRESENTED FOR REVIEW

Whether the district court properly ordered the United States military to allow the federal public defender to meet with the detained enemy combatant in private and without military personnel present.

STATEMENT OF THE CASE

This habeas action, and the related habeas actions pending on appeal before this Court in No. 02-6827, seek the release of Yaser Esam Hamdi, an enemy combatant in the control of the United States military. Hamdi was captured and taken into control of the United States military in Afghanistan in connection with the military campaign that was launched by the President, with the statutory backing of Congress, in the wake of the savage September 11 attacks on this Nation and its citizens. The military has determined that Hamdi should be detained as an enemy combatant in accordance with the laws and customs of war, and he is currently being detained as such at the Naval Station Brig at Norfolk, Virginia. Respondents in this action are the Secretary of Defense and Commander of the Norfolk Naval Brig.

Initial Actions. On May 10, 2002, the federal public defender for the Eastern District of Virginia, Frank W. Dunham, Jr., filed a petition for habeas corpus in the District Court for the Eastern District of Virginia, naming as petitioners Hamdi and the public defender as "next friend" for Hamdi, with whom the public defender concededly has no relationship. Hamdi v. Rumsfeld, E.D. Va. Civ. Action No. 2:02:cv348 (No. 348). On May 24, 2002, a second habeas petition was filed on behalf of Hamdi by Christian A. Peregrim, a non-lawyer, who also has acknowledged that he has no relationship with Hamdi. Hamdi v. United States Navy, E.D. Va. Civ. Action No. 2:02:cv382 (No. 382); see June 3, 2002 Letter from C. Peregrim to District Court (attached to Resps.' Emergency Mot. for Stay Pending Appeal).

On May 29, 2002, following a hearing, the district court entered an order allowing the appointment of the public defender as counsel for Hamdi in the first action, and ordering that such action was properly filed by the public defender as "next friend." May 29 Order at 2-3. The district court further consolidated the first action with the Peregrim action, and ordered respondents to answer the petitions by June 13, 2002. In addition, the district court ordered that "Hamdi must be allowed to meet with his attorney because of the fundamental justice provided under the Constitution of the United States"; that such meeting must be allowed to take place in "private" and "without military personnel present"; and that such "meeting must be

allowed to go forward as of 1 p.m. on Saturday, June 1, 2002." Id. at 3-4.

Respondents appealed the district court's May 29 Order and requested a stay of that order from this Court pending appeal. In particular, respondents argued that the district court lacked jurisdiction to issue its May 29 Order, because neither the public defender nor Peregrim has "next-friend" standing to file a habeas petition on behalf of Hamdi, see Whitmore v. Arkansas, 495 U.S. 149 (1990), and that the district court's access order was premature and unfounded on the merits. See No. 02-6827 Resps.' Emergency Mot. for Stay Pending Appeal at 8-16. On May 31, 2002, a panel of this Court (Chief Judge Wilkinson, with the concurrence of Judge Wilkins and Judge Traxler) issued a stay of the district court's order until "further order of this Court," and scheduled oral argument on the district court's order for June 4, 2002. The argument was held on June 4, and the appeal (No. 02-6827) remains pending.[1]

This Action. On June 11, 2002, while the appeal in No. 02-6827 was pending, the district court issued an order in a third habeas action filed on behalf of Hamdi, this time by Hamdi's father, Esam Fouad Hamdi, as "next friend." Hamdi v. Rumsfeld, E.D. Va. Civ. Action No. 2:02:cv439 (No. 439). Before respondents had been served

[1] As explained in respondents' stay motion in this appeal (at 7 & n.5), neither the district court's June 11 Order nor the filing of the latest habeas petition moots the appeal in No. 02-6827, or in any way lessens the need for this Court's resolution of the important jurisdictional issues raised by that appeal.

with the petition (or had any notice of it), the district court found that Hamdi's father "is a proper next friend" and ordered "the petition filed." June 11 Order at 2. The court further ordered the consolidation of the new action with the prior actions, while stating that, "[i]t further appearing that the matters involved in this case are currently on appeal before the United States Court of Appeals for the Fourth Circuit," the consolidation was "subject to the [Fourth Circuit] allowing such consolidation." Id. at 2 (emphasis added). The court also ordered, pursuant to 18 U.S.C. 3006A, the appointment of the public defender as "counsel for the Petitioner." Id. at 2-3.

In addition, the district court ordered that, "for the same reasons articulated in [its] May 29, 2002 Order," respondents were required to allow the public defender to meet with Hamdi in "private * * * without military personnel present." June 11 Order at 3. The court stated that such private, unmonitored access to Hamdi was required "within seventy-two hours of the entry of this Order or immediately following the elimination of any stay of this Order." Ibid. However, the court stayed its June 11 Order "until 5:00 p.m. on Friday June 14, 2002 to allow the Respondents an opportunity to appeal this Order, or if the United States Court of Appeals for the Fourth Circuit allows the consolidation of this matter with the other pending cases, until further Order of the Court of Appeals." Id. at 3-4. Finally, the court ordered respondents to answer the consolidated petitions by June 17, 2002. Id. at 3.

On June 13, 2002, respondents appealed the district court's June 11 Order, and filed an emergency motion for stay pending appeal of that order. That same day, this Court issued a temporary stay to consider respondents' stay motion. On June 14, 2002, the Court issued an order staying the district court's June 11 Order and "all proceedings before the district court in connection with this detainee until resolution of this appeal and appeal No. 02-6827." In addition, the Court directed the parties to brief the merits of the instant appeal.

STATEMENT OF FACTS

On September 11, 2001, the al Qaida terrorist network launched a large-scale attack on the United States, killing approximately 3,000 persons, and specifically targeting the Headquarters of the Nation's Department of Defense. The September 11 attacks inflicted the loss of more American lives than the attack at Pearl Harbor, and were followed by a major military response. Shortly after the attacks, Congress authorized the President to use "force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons." Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001). In authorizing such force, Congress emphasized

that the forces responsible for the September 11 attacks pose an "unusual and extraordinary threat to the national security and foreign policy of the United States," and that "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States." Ibid.

The President, acting pursuant to his authority as Commander in Chief and with express congressional support, dispatched the armed forces of the United States to Afghanistan to seek out and subdue the al Qaida terrorist network and the Taliban regime that had supported and protected that network. The ongoing military operations in Afghanistan – which are being conducted not only by thousands of men and women of the United States armed forces, but also by coalition forces of our international allies and members of the Northern Alliance and other local forces – have resulted, inter alia, in the destruction of al Qaida training camps, removal of the Taliban regime that supported al Qaida, and gathering of vital intelligence concerning the plans, operations, and workings of al Qaida and its supporters. Numerous members of the military forces sent to Afghanistan have lost their lives, and many others have suffered casualties as part of the campaign, which remains active and ongoing. See generally www.army.mil/enduringfreedom.

In the course of the military campaign, United States and allied forces have captured or taken control of thousands of enemy combatants. Consistent with the

settled laws and customs of war (see Part II.A, infra), and with the practice followed in virtually every other major armed conflict in the Nation's history, the United States military has determined to detain many of the enemy combatants captured in Afghanistan. Such detention serves the obvious yet vital objective of preventing combatants from continuing to aid our enemies. In addition, the detention of such enemy combatants is critical to gathering intelligence in connection with the overall war effort in order to aid military operations and prevent additional attacks on the United States or its allies. See Affidavit of Col. Donald D. Woolfolk (Woolfolk Aff.), attached to Resps.' Emergency Mot. for Stay.

The detainee at issue in this case, Yaser Hamdi, was seized as an enemy combatant and taken into control of the United States military in Afghanistan, after the Taliban unit he was with surrendered. The military determined that Hamdi should be detained as an enemy combatant with potential intelligence value. Hamdi was transported by the United States military from Afghanistan to the Naval Base at Guantanamo Bay, Cuba, and was later transferred to the Naval Brig in Norfolk, Virginia, where he is currently detained. Hamdi appears to be a Saudi national who, records indicate, was born in Louisiana. "Hamdi's background and experience, particularly in the Middle East, Afghanistan, and Pakistan, suggest considerable knowledge of Taliban and al Qaida training and operations." Woolfolk Aff. at 2.

SUMMARY OF ARGUMENT

I. The extraordinary context in which this case arises informs virtually every aspect of the controversy before this Court. As this Court has observed, "[o]f the legion of governmental endeavors, perhaps the most clearly marked for judicial deference are provisions for national security and defense." Tiffany v. United States, 931 F.2d 271, 277 (4th Cir. 1991). This case involves a challenge to the actions of the Commander in Chief and the military in providing for the "national security and defense" by capturing and detaining enemy combatants in war time. The challenged exercise of authority falls within the President's core war powers, comes with the statutory authorization of Congress, and directly implicates vital national security interests in defending the Nation against an unprincipled, unconventional, and savage enemy. All the traditional sign posts, in short, call for a court to act with special care in reviewing the challenge in this case. The district court below, however, has approached this case (and the actions on appeal in No. 02-6827) in just the opposite fashion. In doing so, it has issued an order – requiring the United States military to provide an attorney with private and unmonitored access to a captured enemy combatant – that not only is unprecedented, but has no foundation at all.

II. The district court's access order is flawed on several different levels. First, at the most basic level, the question whether an attorney is entitled to meet with

a detained enemy combatant is bound up with that individual's status as an enemy combatant. As explained below, it is well-settled that the military has the authority to capture and detain individuals whom it has determined are enemy combatants in connection with hostilities in which the Nation is engaged, including enemy combatants claiming American citizenship. Such combatants, moreover, have no right of access to counsel to challenge their detention.

Second, at a bare minimum, the district court's access order in this case was fatally premature. The district court ordered that the public defender could have unfettered access to the enemy combatant immediately upon the filing of the public defender's habeas petition on the detainee's behalf – before the court had even evaluated the government's return. As the habeas statute itself recognizes, however, a habeas petition may raise "only issues of law." 28 U.S.C. 2243. In the return, the government may point out dispositive defects in a habeas petition (such as lack of jurisdiction) that necessitate dismissal of the petition at the outset of the action. Similarly, after the return is filed, it may be apparent that the only issues to be resolved are legal in nature, for example, whether the existence, or not, of a congressional declaration of war negates the government's authority to capture and detain enemy combatants. The indisputable fact that any given habeas petition may be disposed of solely on the papers on questions of law (which would obviate any need for access)

is, in itself, a sufficient reason for this Court to overturn the district court's order requiring the United States military to provide an attorney with access to an enemy combatant upon the mere filing of a habeas action.

Third, courts have an extremely narrow role in reviewing the adequacy of the government's return in a habeas action, such as this, challenging the quintessentially military judgment to detain an individual as an enemy combatant in a time of war. A court's inquiry should come to an end once the military has shown in the return that it has determined that the detainee is an enemy combatant. Although counsel may argue that that status is not a legally sufficient reason to justify the individual's detention (a flawed argument in light of the military's clear authority to detain such enemy combatants), the Court may not second-guess the military's enemy-combatant determination. At the very most, given the separation of constitutional powers in this unique area, a court could only require the military to point to some evidence supporting its determination. Either way, no evidentiary hearing is required to dispose of a habeas petition in this military context.

Finally, the district court's premature access order unnecessarily jeopardizes compelling national security interests in at least two basic respects. First, mandating private access to counsel for enemy combatants is likely to interfere with if not irreparably harm the military's ongoing efforts to gather intelligence that may protect

American interests and lives in the war effort and help protect the home front from further attacks. The moment that counsel is inserted between an enemy combatant and his captors, the relationship of dependency on which fruitful interrogation depends may be destroyed. Second, the enemy in the current war has trained its members, and in all likelihood its supporters, to pass concealed messages through unwitting intermediaries if they are taken into custody. Before issuing its order, the district court in this case did not provide the government with any opportunity to be heard with respect to the national security interests against allowing attorney access to enemy combatants. That failure, alone, is reversible error.

III. The district court's June 11 Order suffers from two additional errors. First, the district court erred in purporting to consolidate this habeas action with the prior habeas actions on appeal in No. 02-6827, and in issuing another access order – in the same "consolidated" action – while the validity of the district court's initial access order was pending before this Court in No. 02-6827. Second, the district court erred in appointing the federal public defender as counsel for the enemy combatant, pursuant to 18 U.S.C. 3006A, without adequately inquiring into the necessity of requiring the taxpayers to pay for that representation. Those errors underscore the district court's departure in this case from the customary manner in which courts approach challenges in sensitive constitutional areas, such as military affairs.

STANDARD OF REVIEW

This Court reviews de novo the entry of a preliminary injunction when, as here, the propriety of that decision raises only a legal question. Commodity Futures Trading Comm'n v. Kimberlynn Creek Ranch, Inc., 276 F.3d 187, 191 (4th Cir. 2002); accord Eisenberg v. Montogomery County Pub. Schs., 197 F.3d 123, 128 (4th Cir. 1999), cert. denied, 529 U.S. 1019 (2000); NationsBank Corp. v. Herman, 174 F.3d 424, 428 (4th Cir.), cert. denied, 528 U.S. 1045 (1999).

ARGUMENT

THE DISTRICT COURT'S JUNE 11 ORDER SHOULD BE SET ASIDE

I. THE DISTRICT COURT IMPROPERLY DISREGARDED SETTLED PRINCIPLES OF JUDICIAL RESTRAINT IN REVIEWING THE EXERCISE OF CORE CONSTITUTIONAL WAR POWERS

The Constitution vests the President with exclusive authority to act as Commander in Chief and as the Nation's sole organ in foreign affairs. See U.S. Const. Art. II, § 2; Dames & Moore v. Regan, 453 U.S. 654, 660-661 (1981); United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 320 (1936); The Prize Cases, 67 U.S. (2 Black) 635, 670 (1862); Madsen v. Kinsella, 188 F.2d 272, 274 (4th Cir. 1951), aff'd, 343 U.S. 341 (1952). This case directly involves the President's core functions as Commander in Chief in wartime: the capture, detention, and treatment of the enemy and the collection and evaluation of intelligence vital to national security.

Furthermore, the President here is acting with the added measure of the express statutory backing of Congress. See Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001); Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635-637 & n.2 (1952) (Jackson, J., concurring).

Courts are normally circumspect when asked to act in disputes that touch upon or may interfere with sensitive matters of foreign policy or national security. See, e.g., Dames & Moore v. Regan, 453 U.S. at 660-661; see also Youngstown Sheet & Tube Co., 343 U.S. at 635 (Jackson, J., concurring). And of particular importance here, courts have long handled challenges to the conduct of military operations with special care and, indeed, have concluded that numerous areas of military affairs are not amenable to judicial review at all. See, e.g., Stewart v. Kahn, 78 U.S. 493, 506 (1870); United States v. The Three Friends, 166 U.S. 1, 63 (1897); The Prize Cases, 67 U.S. (2 Black) at 670; see also Tiffany v. United States, 931 F.2d 271, 275 (4th Cir. 1991) ("Because providing for the national security is both a duty and a power explicitly reserved by the Constitution to the executive and legislative branches of government, the judiciary must proceed in this case with circumspection."), cert. denied, 502 U.S. 1030 (1992).

In Thomasson v. Perry, 80 F.3d 915, 924-926 (4th Cir.), cert. denied, 519 U.S. 948 (1996), this Court reviewed in depth the constitutional, historical, and practical

reasons that the courts – in accordance with their assigned constitutional role – act with great deference when called upon to review the exercise of military powers by the President and Congress, as well as by the military personnel "who 'have been charged by the Executive and Legislative Branches with carrying out our Nation's military policy.'" Id. at 926. Thomasson involved a challenge to the "exercise of military authority" in peacetime. Id. at 919-920. The fundamental considerations that framed the Court's analysis in Thomasson apply with equal, if not much greater, force to the challenged exercise of military authority at issue here – i.e., the capture and detention of the enemy in a time of active war.

Indeed, in Johnson v. Eisentrager, 339 U.S. 763, 779 (1950), the Supreme Court recognized the unique concerns inherent in entertaining habeas petitions filed on behalf of enemies held by our military in time of hostilities:

> The writ, since it is held to be a matter of right, would be equally available to enemies during active hostilities as in the present twilight between war and peace. Such trials would hamper the war effort and bring aid and comfort to the enemy. They would diminish the prestige of our commanders, not only with enemies but with wavering neutrals. It would be difficult to devise a more effective fettering of a field commander than to allow the very enemies he is ordered to reduce to submission to call him to account in his own civil courts and divert his efforts and attention from the military offensive abroad to the legal defensive at home. Nor is it unlikely that the result of such enemy litigiousness would be a conflict between judicial and military opinion highly comforting to enemies of the United States.

Those same concerns are pressing here, and frame the nature of the habeas

litigation now before this Court in this appeal and in No. 02-6827. While this case does not come within the strict application of Eisentrager's jurisdictional rule, the fact that the detainee at issue in this case – unlike those in Eisentrager – claims American citizenship and is now being held by the military in this country does not lessen the concerns identified in Eisentrager with allowing judicial interference with ongoing military operations: diminishing the prestige of our commanders; diverting their attention from the war effort and possibly requiring them to return from abroad to be called into account in our courts; and risking a conflict of military and judicial opinion. The same considerations that led the Court to find habeas completely unavailable in Eisentrager limit the scope of the writ here and counsel in favor of deference to military judgments here. Moreover, the litigation in this case raises the added risk – underscored by the judicial orders at issue in this appeal and in No. 02-6827 – of interfering with a critical component of the ongoing military campaign: gathering intelligence from our enemies to aid in prosecuting the overall war effort.[2]

Nonetheless, far from approaching this litigation with the customary deference accorded by the courts in reviewing matters affecting national security and ongoing

---

[2] The ongoing nature of hostilities underscores the need for deference to military judgments. Even the dissenters in Eisentrager recognized the perils of judicial second-guessing of active military operations. See 339 U.S. at 796 (Black, J., dissenting).

military operations, the district court has repeatedly demonstrated the opposite tendency. In the first two habeas petitions now on appeal in No. 02-6827, the district court disregarded as "technicalities" (see May 29 Order at 3) the clear jurisdictional defects tainting those petitions – which divested the court of any authority to act with respect to those petitions – and it took the unprecedented step of ordering the United States military to allow an attorney to have private and unmonitored access to an enemy combatant in the very earliest stages of the litigation, before the government had even filed a return explaining why the detainee is being lawfully held.

In the present action, the district court went even further. While the same matters were pending on appeal to this Court in No. 02-6827, the district court purported to consolidate the new petition filed on behalf of the detainee with the jurisdictionally flawed petitions in No. 02-6827, and to issue another access order – with a new 72-hour deadline – requiring the United States military to provide the public defender with private and unmonitored access to the detainee. June 11 Order at 2-3. What is more, the district court did so sua sponte, immediately upon the filing of the new petition – before the government had even been served with the petition, much less had an opportunity to answer it. And the district court took these unprecedented steps despite the fact that the latest habeas petition filed by the public defender – unlike the initial petition, which specifically requested the district court to "Order

Respondents to permit counsel to meet and confer with Mr. Hamdi in private and unmonitored communications," No. 348 Pet. at 7 – omits any request for access.

As explained below, the district court's extraordinary access order is without precedent or foundation. But equally important, the district court's actions contradict the necessary and customary deference exercised by the courts when asked to intervene in sensitive constitutional areas and, in particular, when asked to review military decisions in a time of war. In resolving this appeal, the Court should make clear the appropriate framework for the lower courts to apply in considering matters with such national security implications, i.e., the framework set forth in this Court's en banc decision in Thomasson. See 80 F.3d at 924-926. The district court's actions to date in this litigation are far removed from that paradigm.

II. THE DISTRICT COURT ERRED IN ORDERING RESPONDENTS TO PROVIDE THE PUBLIC DEFENDER WITH PRIVATE AND UNMONITORED ACCESS TO THE DETAINEE

In failing to approach this case with the traditional care exercised by the courts in reviewing challenges to military decisions, the district court issued an extraordinary mandate – requiring the military to provide an enemy combatant with private and unmonitored access to counsel – that not only is unprecedented but is the product of several distinct legal errors requiring reversal of that order.

A. Under Settled Law, Enemy Combatants Are Subject To Detention Without Access To Counsel To Challenge Their Detention

1. It is well-settled that the United States military may seize and detain enemy combatants, or other belligerents, at least for the duration of a conflict. For example, in Ex parte Quirin, 317 U.S. 1, 30-31 (1942) (emphasis added and footnotes omitted), the Supreme Court stated as follows:

> By universal agreement and practice, the law of war draws a distinction between the armed forces and the peaceful populations of belligerent nations and also between those who are lawful and unlawful combatants. Lawful combatants are subject to capture and detention as prisoners of war by opposing military forces. Unlawful combatants are likewise subject to capture and detention, but in addition they are subject to trial and punishment by military tribunals for acts which render their belligerency unlawful.

See also id. at 31 n.8 (citing authorities); Duncan v. Kahanamoku, 327 U.S. 304, 313-314 (1946); In re Territo, 156 F.2d 142, 145 (9th Cir. 1946); Ex parte Toscano, 208 F. 938, 940 (S.D. Cal. 1913); L. Oppenheim, International Law 368-369 (H. Lauterpacht ed., 7th ed. 1952).[3]

As the court of appeals explained in the Territo case, "[t]he object of capture is to prevent the captured individual from serving the enemy. He is disarmed and from

---

[3] The practice of capturing and detaining enemy combatants is as old as war itself. See A. Rosas, The Legal Status of Prisoners of War 44-45 (1976). In modern conflicts, the practice of detaining enemy combatants and hostile civilians generally has been designed to balance the humanitarian purpose of sparing lives with the military necessity of defeating the enemy on the battlefield. Id. at 59-80.

then on he must be removed as completely as practicable from the front, treated humanely, and in time exchanged, repatriated, or otherwise released." 156 F.2d at 146 (footnotes omitted). The capture and detention of enemy combatants also serves other vital military objectives, including the critical and age-old objective of obtaining intelligence from captured combatants to aid in the war effort. See Woolfolk Aff. at 2. At the same time, once individuals are taken into control as enemy combatants, they are protected from harm or other reprisals, given medical care and treated humanely, and may be visited by the International Committee of the Red Cross.

It also is settled that the military's authority to detain an enemy combatant is not diminished by a claim, or even a showing, of American citizenship. See, e.g., Quirin, 317 U.S. at 37 ("Citizenship in the United States of an enemy belligerent does not relieve him from the consequences of a belligerency which is unlawful"); In re Territo, 156 F.2d at 144 ("[I]t is immaterial to the legality of petitioner's detention as a prisoner of war by American military authorities whether petitioner is or is not a citizen of the United States of America."); Colepaugh v. Looney, 235 F.2d 429, 432 (10th Cir. 1956) ("[T]he petitioner's citizenship in the United States does not * * * confer upon him any constitutional rights not accorded any other belligerent under the laws of war."), cert. denied 352 U.S. 1014 (1957). To be sure, the fact that a detainee has American citizenship may enable him to proceed with a habeas action that could not be brought

by an alien (cf. Eisentrager), but it does not affect the military's settled authority to detain him once it has determined that he is an enemy combatant.

The United States military has captured and detained enemy combatants during the course of virtually every major conflict in the Nation's history, including more recent conflicts such as the Gulf, Vietnam, and Korean wars. It plainly has authority to do so in connection with the present conflict as well.

2. There is no right under the laws and customs of war for an enemy combatant to meet with counsel concerning his detention, much less to meet with counsel in private, without military authorities present. That is true with respect to enemy combatants who are captured and detained on the battlefield in a foreign land; enemy combatants who are captured overseas and brought to the United States for detention (like hundreds of thousands of prisoners of war during World War II); and enemy combatants who are captured and detained in this country (like the saboteurs in Quirin). Even under the Third Geneva Convention – which does not afford protections to unlawful enemy combatants, such as the detainee here – prisoners of war have no right of access to counsel to challenge their detention. See Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T.

3317, 75 U.N.T.S. 135 (GPW), Article 105.[4]

The Constitution does not supply any different guarantee. The Sixth Amendment by its terms applies only in the case of "criminal prosecutions," U.S. Const. amend. VI, and therefore does not apply to the detention of any enemy combatant who – like the vast majority of such combatants – has not been charged with any crime. Cf. Middendorf v. Henry, 425 U.S. 25, 38 (1976) ("[A] proceeding which may result in deprivation of liberty is nonetheless not a 'criminal proceeding' within the meaning of the Sixth Amendment if there are elements about it which sufficiently distinguish it from a traditional civilian criminal trial."). Similarly, the Self-Incrimination Clause of the Fifth Amendment is a "trial right of criminal defendants," and therefore also does not extend to this situation. United States v. Verdugo-Urquidez, 494 U.S. 259, 264 (1990) (emphasis added). The only possible remaining source of such an access right is the Due Process Clause.

Any suggestion of a generalized due process right under the Fifth Amendment could not be squared with, inter alia, the historical unavailability of a right of access to

---

[4] Article 105 of the GPW provides that a prisoner of war should be provided with counsel to defend against charges brought against him in a trial proceeding at least two weeks before the opening of such trial. But the availability of that general trial right only underscores that prisoners of war who do not face such charges are not entitled to counsel, or access to counsel, simply to challenge the fact of their wartime detention.

counsel by those held as enemy combatants in similar circumstances. Cf. Herrera v. Collins, 506 U.S. 390, 407-408 (1993); Medina v. California, 505 U.S. 437, 445-446 (1992); Moyer v. Peabody, 212 U.S. 78, 84 (1909); see also Colepaugh, 235 F.2d at 432; Ex parte Toscano, 208 F. at 943. Indeed, as the Supreme Court emphasized in Quirin, 317 U.S. at 27-28, "[f]rom the very beginning of its history this Court has recognized and applied the law of war as including that part of the law of nations which prescribes, for the conduct of war, the status, rights and duties of enemy nations as well as of enemy individuals." Moreover, in conducting such a due process analysis under the Fifth Amendment, the Court would have to balance the creation of such a right of access against the government's own interests, including the President's plenary authority as Commander in Chief and the important national security interests implicated by allowing access to counsel to enemy combatants.

In Middendorf v. Henry, 425 U.S. at 42-43, for example, the Supreme Court rejected the argument that "the due process standards of the Fifth Amendment" required that servicemen be entitled "to counsel in summary court-martial proceedings," even though, the court recognized, individuals subject to such proceedings "may be subjected to loss of liberty." In undertaking its Fifth Amendment analysis, the Court emphasized at the outset that whether due process "embodies a right to counsel [in such circumstances] depends upon an analysis of the

interests of the individual and those of the regime to which he is subject." Id. at 43. More to the point, in concluding that no generalized right to counsel attached in such circumstances, the Court emphasized the unique interests of the military in avoiding the addition of counsel to such court-martial proceedings. See id. at 45-46; id. at 49-51 (Powell, J., joined by Blackmun, J., concurring).

Moreover, the Supreme Court has rejected the argument that due process entitles state prisoners to counsel in seeking post-conviction relief, even in capital cases. See Pennsylvania v. Finley, 481 U.S. 551 (1987); Murray v. Giarratano, 492 U.S. 1 (1989) (plurality opinion); see also United States v. Gouveia, 467 U.S. 180 (1984) (no right to counsel during period of administrative detention). Likewise, there is no tradition or practice of providing those held as enemy combatants with access to counsel to challenge their detention by way of a habeas action. Indeed, at least at common law, "a prisoner of war has no standing to apply for the writ of habeas corpus." R.J. Sharpe, The Law of Habeas Corpus 112 (1976) (citing authorities). To be sure, in more recent times, courts have entertained habeas petitions filed on behalf of those held in this country as enemy combatants. See, e.g., Territo, supra. But as explained below, the scope of review in those proceedings is limited, and does not support the creation of a "due process" right of access to counsel in this context.

Accordingly, even the most general due process analysis does not support the

creation of the sort of free-floating right of an enemy combatant to access to counsel recognized by the district court. But in any event, even assuming that the Fifth Amendment did confer upon enemy combatants some right of access to counsel to challenge their detention (or, indeed, a right of counsel to have access to someone being detained as an enemy combatant), such a right would be available only to the extent that it was necessary to enable a court to resolve a proper habeas petition, and only to the extent that recognizing such a right did not unduly burden the compelling interests of the President as Commander in Chief or the military in detaining captured enemy combatants. In other words, any such right would take its form from the constitutional, procedural, and national security limitations on a habeas proceeding in this particular context. As explained below, an analysis of those factors demonstrates that the access order at issue in this case must be set aside.[5]

---

[5] The public defender states that "[t]he District Court ordered that Respondents provide access to Petitioner pursuant to its authority to appoint counsel under 18 U.S.C. 3006A. Appellees' Resp. to Resps.' Emergency Mot. to Stay at 5 (emphasis added). That is incorrect. In its June 11 Order, the district court ordered access to counsel "for the same reasons articulated in the May 29, 2002 Order." June 11 Order at 3. That is, the district court ordered such access based on "fundamental justice provided under the Constitution of the United States." May 29 Order at 4; see ibid. ("Fair play and fundamental justice require nothing less."). In any event, as explained below, the public defender was not properly appointed in this case under Section 3006A. Moreover, even if his appointment were proper, nothing in the text or history of Section 3006A suggests that Congress sought to confer upon detainees (or properly appointed counsel) a

B. At A Bare Minimum, The District Court's Access Order Was Entirely Premature In The Context Of This Habeas Proceeding

Putting to one side the constitutional and practical limitations on a habeas proceeding of this kind (see infra), the district court's access order is insupportable from a purely procedural standpoint. The district court ordered the United States military to provide the public defender with private, unmonitored access to an enemy combatant based solely on the filing of this habeas petition – before even evaluating the government's return. As is true in any habeas action, however, the government's return might make clear either that the petition must be dismissed or that "only issues of law" remain in adjudicating the writ. 28 U.S.C. 2243. In either event, there would be no need for any evidentiary proceedings. See Walker v. Johnston, 312 U.S. 275, 284 (1941) (a court may find on the face of the pleadings in a habeas action "that no issue of fact is involved"; "useless grant of the writ * * * may be avoided where from undisputed facts or incontrovertible facts * * * it appears, as a matter of law, no cause for granting the writ exists"). That understanding is consistent with the special role assigned by the habeas statute to the answer or return. 28 U.S.C. 2248.

---

right to the extraordinary type of access to counsel mandated by the district court in this case. And even if there were any basis to argue a contrary position, the longstanding constitutional-avoidance canon of construction would counsel strongly against interpreting Section 3006A in that manner.

For example, as the pending petitions in No. 02-6827 illustrate, a habeas petition filed on behalf of an individual being detained as an enemy combatant might be jurisdictionally defective at the outset. A return pointing out such a defect would eliminate the need for any further proceedings, including any evidentiary proceedings. Similarly, a habeas petition asserting that an enemy combatant is not being lawfully detained because he was captured by allied forces, and not United States forces, would raise only the legal question of whether such a distinction made any difference as a matter of law with respect to the military's authority to detain the individual under the laws and customs of war. There are countless other scenarios in which it might be clear with the benefit of the government's return that no evidentiary inquiry at all is required to dispose of a habeas petition. Because it is possible that any given case may be resolved as a matter of law (i.e., in a manner that does not give rise to a need for counsel to meet with the detainee), a right of access to counsel cannot be triggered by the mere filing of a habeas petition on behalf of an enemy combatant.

Indeed, in Gagnon v. Scarpelli, 411 U.S. 778, 790 (1973) – the high water mark of due process in the right-to-counsel context – the Court refused to adopt an automatic right to counsel covering parole and probation revocation hearings. Instead, the Court adopted a "case-by-case" approach, reasoning that "[a]lthough the presence and participation of counsel will probably be both undesirable and constitutionally

unnecessary in most revocation hearings, there will remain certain cases in which" the Fifth Amendment requires that such counsel be provided. Ibid. (emphasis added). In Middendorf, the Supreme Court declined to extend Gagnon to the "military context." 425 U.S. at 43. Yet, the district court's access order in this case goes even further than the due process rationale of Gagnon. The district court ordered access based on the mere filing of the petition before there was any practical opportunity to evaluate the desirability or necessity of conferring a right of access to counsel in this proceeding.

Moreover, in ordering such immediate access to counsel, the district court all but presumed that the government is detaining an individual in violation of law, when the customary burden of proof in habeas proceedings is just the opposite, see Garlotte v. Fordice, 515 U.S. 39, 46 (1995), and when, regardless of the conventional burden, there are compelling separation of powers and national security concerns that demand careful consideration of and in most if not all cases deference to the government's response. The timing of the district court's access order is itself ground for reversal.

C. There Is No Basis For Ordering Attorney Access In Resolving A Habeas Petition Filed On Behalf Of An Enemy Combatant

1. In any event, regardless of the question of timing, given the constitutionally limited role of the courts in reviewing military decisions, courts may

not second-guess the military's determination that an individual is an enemy combatant and should be detained as such. Thus, no evidentiary proceedings are required to resolve a habeas petition filed on behalf of such a detainee and no access between the detainee and counsel for the next-friend is necessary.

As this Court has stated, "the lack of competence on the part of the courts [with respect to military judgments] is marked." Thomasson, 80 F.3d at 926 (quoting Rostker v. Goldberg, 453 U.S. 57, 65 (1981)) (bracketed material added in Thomasson); accord Berry v. Bean, 796 F.2d 713, 716-717 (4th Cir. 1986). This case involves a challenge to one of the most fundamental military judgments of all: the determination that someone who was captured in the theater of battle is an enemy combatant and should be detained as such. See Hirota v. MacArthur, 338 U.S. 197, 215 (1949) ("[T]he capture and control of those who were responsible for the Pearl Harbor incident was a political question on which the President as Commander-in-Chief, and as spokesman for the nation in foreign affairs, had the final say.") (Douglas, J., concurring); see also Ludecke v. Watkins, 335 U.S. 160, 170 (1948) (determinations with respect to how to treat enemy aliens "when the guns are silent but the peace of Peace has not come * * * are matters of political judgment for which judges have neither technical competence nor official responsibility"); Eisentrager, 339 U.S. at 789 ("Certainly it is not the function of the Judiciary to entertain private

litigation – even by a citizen – which challenges the legality, the wisdom, or the propriety of the Commander-in-Chief in sending our armed forces abroad or to any particular region.").[6]

Especially in a time of active conflict, a court considering a properly filed habeas action generally should accept the military's determination that a detainee is an enemy combatant. Going beyond that determination would require the courts to enter an area in which they have no competence, much less institutional expertise, intrude upon the constitutional prerogative of the Commander in Chief (and military authorities acting at his control), and possibly create "a conflict between judicial and military opinion highly comforting to enemies of the United States." Eisentrager, 339 U.S. at 779. See also Tiffany, 931 F.2d at 278 ("Not only do courts lack the expertise to evaluate military tactics, but they will often be without knowledge of the facts or standards upon which military decisions have been based.").[7]

---

[6] In a similar vein, Charles Evans Hughes observed that the "war power of the national government is the power to wage war successfully." C. Hughes, War Powers Under the Constitution, 42 A.B.A. Rep. 232, 238. Thus, he continued, it is "not for any court to sit in review of the wisdom of the actions of the Executive or of Congress, or to substitute its judgment for theirs. If the Court could say there was a rational basis for the military decision, it would be sustained." Ibid.

[7] Congress's joint resolution authorizing the use of military force in response to the September 11 attacks is specifically framed in terms of taking action against that the "nations, organizations, or persons [that] he [i.e., the President] determines planned, authorized, committed, or aided the terrorist attacks that occurred on

That conclusion does not nullify the writ.[8] As explained above, although a court should accept the military's determination that an individual is an enemy combatant, a court may evaluate the legal consequences of that determination. For example, a court might evaluate whether the military's determination that an individual is an enemy combatant is sufficient as a matter of law to justify his detention even if the combatant has a claim to American citizenship. See Territo, supra. In doing so, however, a court may not second-guess the military's determination that the detainee is an enemy combatant, and therefore no evidentiary proceedings concerning such determination are necessary.[9]

September 11, 2001, or harbored such organizations or persons." 115 Stat. 224 (2001) (emphasis added). Although it falls within his core functions as Commander in Chief, the capture and detention of enemy combatants in connection with the ongoing military campaign is also a vital and common sense component of the military force backed by Congress.

[8] That is certainly true as a historical matter. One of the principal purposes of the writ was to require the executive to explain why it was holding an individual, and not for a court to second-guess the facts underlying that determination. See, e.g., C. Forsythe, The Historical Origins of Broad Federal Habeas Review Reconsidered, 70 Notre Dame L. Rev. 1079, 1094 (1995) ("At common law, the allegations in the 'return' were deemed conclusive and could not be controverted by the prisoner."); D. Oaks, Legal History in the High Court – Habeas Corpus, 64 Mich. L. Rev. 451, 453 (1966).

[9] In In re Yamashita, 327 U.S. 1 (1946), the Supreme Court considered the scope of judicial review in a habeas action challenging a prisoner of war's conviction and death sentence before a military commission. In rejecting that petition, the Court "emphasized" at that outset "that on application for habeas

Furthermore, as this Court observed in the Thomasson case, the hands-off approach taken by the courts when it comes to reviewing military decisions or operations does not mean that the war power may be exercised without check:

> [I]t is no surprise that the Founders failed to provide the federal judiciary with a check over the military powers of Congress and the President. See U.S. CONST. art. III. To do so would have placed, in Hamilton's words, a 'constitutional shackle' on the ability of Congress and the President to carry out the duties attendant to national security. Moreover, the virtue of placing military power in the democratic branches was obvious: '[I]f the majority should be really disposed to exceed the proper limits, the community will be warned of the danger [by the minority], and [the community] will have an opportunity of taking measures to guard against it.' Federalist No. 26, at 172 (Alexander Hamilton). The federal judiciary – appointed with life tenure – was not regarded as an appropriate repository for such immense power and accordingly was given 'no influence over either sword or purse.' Federalist No. 78, at 465 (Alexander Hamilton).

80 F.3d at 924. Especially in a case such as this, involving the detention of an enemy combatant who claims American citizenship, the filing of a habeas petition will place

---

corpus [in this situation] we are not concerned with the guilt or innocence of the petitioners." Id. at 8. Rather, the Court continued, "[w]e consider here only the lawful power of the commission to try the petitioner for the offense charged." Ibid. See Eisentrager, 339 U.S. at 797 (Black, J., dissenting) (Judicial review of military charges "is of most limited scope"; "[w]e ask only whether the military tribunal was legally constituted and whether it had jurisdiction to impose punishment for the conduct charged."). Although this case does not involve the trial or punishment of prisoners of war for war crimes, Yamashita supports the conclusion that the Court's review of the instant petition "is of the most limited scope," and is limited to legal issues surrounding the military's authority to detain an individual that it has determined is an enemy combatant.

– and, indeed, has placed – the Executive's actions in the public light. That kind of scrutiny, not judicial scrutiny in a habeas proceeding, was the principal check envisioned by the Framers on any potential Executive abuses in this sphere.

2. At the very most, in light of the fundamental separation of powers and other considerations discussed above, even if it were appropriate for a court to exercise some limited review over the quintessentially military determination that an individual is an enemy combatant, a court's proper role would be solely to confirm that there was some factual basis to support that determination.

In considering habeas challenges to analogous – but much less constitutionally sensitive – executive determinations, courts have refused to permit the use of the writ to challenge the factual accuracy of such determinations, and instead only call upon the executive to provide "some evidence" supporting its determination. See, e.g., INS v. St. Cyr, 533 U.S. 289, 306 (2001) (deportation order: "Until the enactment of the 1952 Immigration and Nationality Act, the sole means by which an alien could test the legality of his or her deportation order was by bringing a habeas corpus action in district court. In such cases, other than the question whether there was some evidence to support the order, the courts generally did not review factual determinations made by the executive.") (emphasis added); Eagles v. United States, 329 U.S. 304, 312 (1946) (selective service determination: "If it cannot be said that there were procedural

irregularities of such a nature or magnitude as to render the hearing unfair, or that there was no evidence to support the order, the inquiry is at an end.") (citations omitted); Fernandez v. Phillips, 268 U.S. 311, 312 (1925) (extradition order: "[H]abeas corpus is available only to inquire whether the magistrate had jurisdiction, whether the offense charged is within the treaty and, by a somewhat liberal extension, whether there was any evidence warranting the finding that there was reasonable ground to believe the accused guilty."); United States v. Commissioner, 273 U.S. 103, 106 (1927) ("Upon a collateral review in habeas corpus proceedings, it is sufficient that there was some evidence from which the conclusion of the administrative tribunal could be deduced."). The focus of the inquiry is the executive's determination, and the court's role is limited to confirming that there was a factual basis for that determination. There no role for the court itself to evaluate the underlying question.

Moyer v. Peabody, 212 U.S. 78 (1909), is also instructive. That case involved a due process challenge brought by an individual who had been detained, without probable cause, for months by the governor of Colorado acting in his capacity of "commander-in-chief of the state forces" during a local "state of insurrection." Id. at 82. In rejecting that challenge, Justice Holmes, writing for a unanimous Court, explained: "So long as such arrests are made in good faith and in the honest belief that they are needed in order to head the insurrection off, the Governor is the final judge

and cannot be subjected to an action after he is out of office on the ground that he had not reasonable ground for his belief." Id. at 85; see also United States v. Salerno, 481 U.S. 739, 748 (1987) ("[I]n times of war or insurrection, when society's interest is at its peak, the Government may detain individuals whom the government believes to be dangerous.") (citing Moyer).

In United States v. Chalk, 441 F.2d 1277, 1281 (4th Cir.), cert. denied, 404 U.S. 943 (1971) (emphasis added), which involved a similar challenge to state action in response to a local insurrection, this Court looked to Moyer and held that "the scope of our review in a case such as this must be limited to a determination of whether the mayor's actions were taken in good faith and whether there is some factual basis for his decision that the restrictions he imposed were necessary to maintain order." See id. at 1282 ("It is enough, we think, that there was a factual basis for the mayor's decision to proclaim the existence of a state of emergency and that he acted in good faith."). Moreover, even in the absence of such exigent circumstances, this Court has taken a similarly deferential approach to reviewing the decisions of military commanders in seeking to maintain discipline and order on a military base. See, e.g., Berry, 796 F.2d at 717, 717 (4th Cir. 1986).

The considerations underlying the limited scope of review of the types of executive determinations discussed above are only magnified in the case of the

Executive's determination to detain an individual as an enemy combatant during a state of active hostilities. Accordingly, at most, in such circumstances, a habeas court should only confirm that the military had any factual basis for its determination that an individual is an enemy combatant. Moreover, because the exclusive focus of the proceedings in such a setting is whether the military's determination has some support in evidence, there is no need for a court to conduct evidentiary hearings with respect to whether that determination is factually disputed by the detainee, or his lawyer. Thus, even under this approach, there would be no need for an attorney to have access to a detained enemy combatant.[10]

D. Allowing Attorney Access To Captured Enemy Combatants Would Threaten Vital National Security Interests

Finally, in considering whether any access to counsel is appropriate in the context of a habeas petition filed on behalf of an enemy combatant, a court also must carefully weigh the government's compelling interest in avoiding such access. As explained in more detail in the Woolfolk Affidavit, permitting counsel to have access, much less private and unmonitored access, to a detained enemy combatant threatens

---

[10] In addition, even in the event that a court found the military's factual basis somehow infirm, the remedy would not be to conduct an evidentiary proceeding in the courts, but rather to allow the military authorities to correct any infirmity. Even under such a highly unlikely scenario, the judicial proceedings would not necessitate access to the detainee.

the national security in at least two basic respects. First, such access would directly interfere with – and likely thwart – ongoing efforts of the United States military to gather and evaluate intelligence about the enemy, its assets, and its plans, and its supporters. Such intelligence is critical to the successful prosecution of any war effort and, in the present conflict, in all likelihood already has avoided additional harm to American lives or interests on the home front. Second, such access may enable detained enemy combatants to pass concealed messages to the enemy about military detention facilities, the security at such facilities, or other military operations – something that members (and presumably supporters) of al Qaida are trained to do.

Collecting and assessing intelligence is one of the most important duties of the Commander in Chief, especially in wartime. See United States v. Marchetti, 466 F.2d 1309, 1315 (4th Cir.) ("[g]athering intelligence information" is "within the President's constitutional responsibility for the security of the Nation as the Chief Executive and as Commander in Chief of our Armed forces"), cert. denied, 409 U.S. 1063 (1972); see also Snepp v. United States, 444 U.S. 507, 512 n.7 (1980) (per curiam) ("It is impossible for a government wisely to make critical decisions about foreign policy and national defense without the benefit of dependable foreign intelligence."). The government's interests in avoiding attorney access to detained enemy combatants, therefore, weigh heavily in any analysis of whether to recognize a right to such access

in habeas proceedings challenging the detention of enemy combatants. The district court below precipitously – and dangerously – dismissed such interests.

III. THE DISTRICT COURT'S JUNE 11 ORDER IS TAINTED BY ADDITIONAL ERRORS

The district court's June 11 Order contains additional defects that further support reversal.

1. The district court erred in purporting to consolidate the instant habeas petition with the petitions currently on appeal in No. 02-6287. As discussed in respondents' stay motion, under the settled rule "[t]he filing of a notice of appeal is an event of jurisdictional significance – it confers jurisdiction on the court of appeals and divests the district court of its control over those aspects of the case involved in the appeal." Griggs v. Provident Consumer Discount Co., 459 U.S. 56, 58 (1982); see United States v. Christy, 3 F.3d 765, 767-768 (4th Cir. 1993) (citing cases). "A district court does not regain jurisdiction until the issuance of the mandate by the clerk of the court of appeals." United States v. Montgomery, 262 F.3d 233, 239-240 (4th Cir. 2001). Although the interlocutory appeal (No. 02-6827) of the district court's May 29 Order did not divest the district court of jurisdiction over the entirety of the underlying habeas petitions, the district court's purported consolidation of this case with the actions in appeal No. 02-6827 is nonetheless error in two different respects.

First, the threshold issue before this Court in appeal in No. 02-6287 is whether the district court had jurisdiction at all with respect to the public defender's and

Peregrim's "next friend" petitions. Although a pending interlocutory appeal may not divest a district court of its jurisdiction with respect to a proposed consolidation in every instance, it should do so where, as here, the central issue on appeal is whether jurisdiction exists in the initial actions. Second, at the same time that it purported to consolidate the cases, the district court awarded precisely the same injunctive relief at issue in No. 02-6287, thereby effectively reentering the same order currently on appeal. See 16 C. Wright et al., Federal Practice and Procedure 3921.2, at 54 (1996) (noting that "power to proceed toward decision of the merits must be distinguished from the power to act on the very order that has been appealed").

Indeed, in issuing its June 11 Order, the district court specifically recognized that "the matters involved in this case are currently on appeal." June 11 Order at 2 (emphasis added). Under the settled rule, the district court therefore lacked "control" (Griggs, 459 U.S. at 58) to act with respect to those matters to the extent that it purported to consolidate this case with the actions appeal in No. 02-6827.

2. The district court also erred in appointing the public defender as "counsel for the Petitioner," by which the district court apparently meant the detainee, pursuant to 18 U.S.C. 3006A. June 11 Order at 3. As In re Heidnik, 112 F.3d 105, 112 (3d Cir. 1997), illustrates, when counsel is appointed in a next-friend situation such as this, it is for the next friend, not for the detainee on whose behalf the next friend seeks

relief. That follows from the text of 18 U.S.C. 3006A, which provides that, "[w]henever * * * the interests of justice so require, representation may be provided for any financially eligible person who * * * is seeking relief under section 2241, 2254, or 2255 of title 28." (Emphasis added.). The detainee himself has not sought relief in this case; indeed, one of the necessary predicates for the detainee's father to maintain this next-friend action is that the detainee himself is unable to seek relief on his own behalf. See Whitmore, 495 U.S. at 163.

Moreover, Section 3006A only authorizes appointment of counsel with respect to a "financially eligible person." The district court found that an affidavit submitted by Hamdi's father was "sufficient evidence of financial eligibility to warrant the appointment of counsel under [18] U.S.C. § 3006A." June 11 Order at 2. That affidavit (Attachment D, Exh. D, to respondents' stay motion), however, states only that Hamdi's father "will be unable to provide funds for the legal services." That loosely worded and unsupported statement does not even amount to a clear assertion that the father lacks the financial resources to pay for counsel, and cannot supply the sole basis for appointment of counsel under Section 3006A. See United States v. Bauer, 956 F.2d 693, 694 (7th Cir. 1992) ("The Criminal Justice Act * * * provides for the appointment of counsel when the judge is 'satisfied after appropriate inquiry that the person is financially unable to obtain counsel.' 18 U.S.C. § 3006A(b). It is

not enough to claim an inability to hire a lawyer and back up the claim with an affidavit; the statute provides for 'appropriate inquiry' into the veracity of the claim."). Indeed, to take one example, the father may only have sworn that he is unable (or disinclined) to federal express or wire funds from overseas.

In any event, even if, in a typical case, language with such wiggle room might suffice for purposes of satisfying Section 3006A's financial-eligibility requirement, it does not do so here. In the course of the actions pending on appeal in No. 02-6827, respondents – in challenging appointment of the same counsel – alerted the district court to press reports indicating that Hamdi's father "holds a prestigious job in a private company in the Jubail Industrial City."[11] Neither the public defender nor the father has ever disputed that report, or sought to explain why, even assuming the father holds such employment, he is financially eligible for the taxpayer-funded services of the public defender to challenge the detention of an enemy combatant. Nevertheless, in appointing the public defender as counsel in this case, the district court never inquired into the matter. That was error. See United States v. Harris, 707 F.2d 653, 661 (2d Cir. 1983) ("[W]here a defendant's inability to afford counsel has been put into doubt, he has the burden of coming forward with evidence," and there is no

[11] A. Almotawa, Saudi seeks release of son from US jail, May 3, 2002 (http://www.arabnews.com/article.asp?sct=esam%20Hamdi&id=14905).

warrant for appointment of counsel if "a defendant fails to come forward with additional evidence instead of relying on a terse form affidavit").

* * * * *

In its June 14 Order, this Court requested the parties to "make plain what action they are requesting that the Court take in this appeal and the reasons for their requests." For the reasons explained above, respondents request the Court to set aside the district court's June 11 Order in its entirety and, in particular, the district court's access order. In addition, as appropriate based on the Court's resolution of this appeal and appeal No. 02-6827, the Court should remand this case with instructions for the district court (1) to conduct any further proceedings necessary with respect to the detainee at issue with the necessary and customary deference exercised by the courts in reviewing military affairs; (2) to require the public defender to show cause why the detainee's father meets the financial eligibility requirements of 18 U.S.C. 3006A, and suspend any further proceedings in this case until a proper showing has been made under Section 3006A; and, if necessary, (3) to permit respondents to file their return to any properly filed habeas petition with respect to the detainee within 5 days of the issuance of this Court's decision, and to refrain from ordering any relief (including access to counsel) until, at a bare minimum, the district court has evaluated the government's return in accordance with the principles set forth

above.

Furthermore, if this Court concludes, for the reasons discussed above, that "precedent dictates a resolution in favor of the government" in this action and that "further remand for consideration on the merits would be futile," the Court not only should dissolve the district court's June 11 injunction, but also remand the case with instructions to dismiss this action outright. Berry v. Bean, 796 F.2d at 719. Given the principles of judicial review set forth above governing the type of habeas action filed in this case on behalf of the detained enemy combatant, and the detainee's status as an enemy combatant, there is no legal basis whatever for granting any of the requested relief in this action. "Though ordinarily a court may not resolve the merits of a dispute on motion for preliminary injunction without notice to the parties, the special circumstances of this case warrant a departure from that requirement." Ibid. The extraordinary, and unfounded, actions taken by the district court to date also support entry of such relief, as an alternative to the prospect of continuing appellate superintending of the district court proceedings.

Finally, in addition to resolving this appeal, the Court should resolve appeal No. 02-6827, and dismiss for lack of jurisdiction the actions pending in that appeal for the reasons explained by respondents in their emergency stay motion in appeal No. 02-6827 and at the oral argument in No. 02-6827.

CONCLUSION

For the foregoing reasons, the district court's June 11 Order should be reversed. In addition, the Court should grant the other relief requested above.

Respectfully submitted,

PAUL J. McNULTY
United States Attorney

PAUL D. CLEMENT
Deputy Solicitor General

ALICE S. FISHER
Deputy Assistant Attorney General

GREGORY G. GARRE
Assistant to the Solicitor General

LAWRENCE R. LEONARD
(757) 441-6331
Managing Assistant United States Attorney

United States Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530-0001

JUNE 2002

○